THE TAMIL NADU
Dr. AMBEDKAR LAW UNIVERSITY
CHENNAI

STUDY MATERIAL

CYBER LAW AND FORENSICS

WORK SUBMITTED TO

THE DIRECTOR, SOEL

Submitted by

Dr. Lucky George

Asst . Professor (SS)

Department of IPR

SOEL, TNDALU

SCHOOL OF EXCELLENCE IN LAW

Cyber law and Forensics

Dr. Lucky George

Assistant Professor(SS)

Department of IPR

SOEL,TNDALU

Preface

The Information and Communication Revolution (ICR), now underway throughout the world, is challenging established institutions and practices in a manner difficult even to comprehend for ordinary folks. The systems of socio-economic organization and political governance are undergoing unprecedented changes compelling Government to review the laws relating to management of knowledge in society.

The industrial revolution has brought about its own set of laws regulating not only business and commercial activity but also the governance of post industrial society. As the industrial revolution affected only certain parts of the world leaving behind the former colonies, the legal systems of the so- called developing countries could not as yet, equip themselves to the challenges of industrialization. Meanwhile, the ICR has overtaken the world, demolishing the economic barriers and political boundaries and challenging the established laws of even the industrialized world. Most developing countries of the world have to make a quantum jump in law making if they want to develop capacities to protect national interests and to avoid exploitation by those who own technology- the limits of which are still unknown.

We can see that after the advent of Internet, in all spheres of life, the regulatory framework analysis has become vital in the era of Digitalization. The course helps in understanding the regulations relating to E-Contracts, E-Taxation, Intellectual Property Issues and Cyber Crimes. The course intended to analyse the need of Cyberspace Regulation both Jurisdiction and Jurisprudential Aspects Of Cyberspace.

Cyber law and Forensics

Course outline

Unit- I
Introduction

Cyber space Introduction and UNCITRAL Model Law - Information Technology Act, 2000 with recent Amendments-jurisdictional Issues- Digital Signatures-Regulation of Certifying Authorities- Cyber Regulation Appellate Tribunal.

Unit- II
Online Contracts

Formation of online Contracts- E-Banking Transactions- Online Payment Options-Online Advertising- Electronic and Digital Signature- Taxation Issues in Cyber Space- Indirect Tax – Tax evasion – Double Tax- International Tax- Permanent Establishment- Protection of Trade secrets and Deceptive trade Practices.

Unit –III
Cyber Crimes

Understanding Cyber Crimes- Actus Reus and Mens Rea-Types of crimes in the internet- Against Person, Against Property, Against Government- Digital Evidence-Investigation and Adjudication of cyber crimes in India- Cyber Arbitration- Cyber Conflict Investigation.

Unit –IV
IPR and Cyber Space

Copyright Issues in the Internet- Protection of computer software- Caching-international regime- OSS-DMCA- Data Protection Directive- Trademark Issues in the Internet- Domain Name- registration –Domain Name Disputes- ICANN-UDRP Policy- Linking- Framing – Meta tagging –database issues in the Internet.

UNIT V
Contemporary Issues

Convergence Technologies- Cloud Computing- Online Digital Libraries – Access to Internet: a Human Right Issue- Issue of Censorship-Privacy Issues- National Security and Social Security.

UNIT -1

INTRODUCTION TO INFORMATION TECHNOLOGY AND CYBER LAWS.

Information technology and cyber space

Concept of information technology

The technology relating to computer systems, their hardware, software and networks, internet, and various applications running on the internet, is broadly referred to as information technology of 'IT'. The Oxford Dictionary defines 'IT' as:

"The study or use of computers, telecommunication systems, and other devices for storing, retrieving and transmitting information."

Concept of Cyber Space

The virtual space in which all of IT-mediated communicated and actions are taking place is often referred to as 'Cyber space'. Cyber space cannot be spatially located. It is made up of intangible objects, such as your website, blog social networks, email accounts, personal information and reputation, Cyberspace can be thought of as a global electronic village with instantaneous communication and no geographical barriers".

The Proliferation of IT and the Need for Regulation of Cyber space.

The proliferation of 'IT' has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems and computer data. The protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others that lawfully utilize those computers, computer systems, and data. The laws governing the physical world are, however, inept at governing transactions in cyber space where the subject matter often is an intangible object such as one's email or Facebook account or website or virtual currency or personal information. The regulation of the cyber space, thus, requires specialized laws.

Cyber Laws

Limitations of Traditional Law and Need for a Separate Law for Cyber Crime

Traditional laws pose several constraints in dealing with cyber-crimes:

(i) **Jurisdictional Issues:**

Cyberspace has no geographic boundaries. A cybercrime may be committed using a computer system or network located in another country. Where the Indian Penal Code 1860 provides for both territorial and extra-territorial jurisdiction. Its extra-territorial jurisdiction is limited to offences committed by Indian citizens. This leaves ambiguity in the applicability of the penal code to cyber offences that may be committed by foreign nationals overseas, but, in a way their impact is felt in India. This 'transnational' element of cybercrime also requires greater international cooperation investigation of offences in other countries and arrest of cybercriminal of other nationalities will require established treaties and special permissions.

(ii) **Inapplicability of Conventional Definitions:** Most crimes in cyberspace involve intangible objects. This creates problems where conventional definitions of crime are involved. For instance, the definition of trespass requires actual physical entry for conviction. Constructive entry upon the property is not within the meaning of this section. In the case of cyber trespass, or hacking where - there is no actual entry into the physical territory where the computer is located this definition would fail. Similarly, the offence of theft is made out when there exists an intent to remove for possession. Therefore, for data to be stolen, it would have to be removed from possession of the owner. If the offender were to simply copy the data onto a pen drive without erasing or modifying the original data in any way, then it may not constitute 'theft' under the traditional definition of the term.

(iii) **Creation of New Crimes:** Cyber space has given birth to several new crimes which are not recognized by conventional laws. For Example, a website can handle only a fixed number of viewer or request (for information) at a given point of time. A cyber-criminal an prevent the website from functioning by overloading it with requests (known as a denial of service attack). This kind of attack can cause huge losses to an online business, but, there would be no clear remedy under ordinary law. Similarly, the Act elevates the offence of denial of access and introducing computer viruses with the intent of striking terror in a section of people to the status of 'cyber-terrorism' and provides for significant punishment for the same. Under section 66F the IT Act, the provision relating to cyber-terrorism, is worded similar to Section 3 of the Prevention of Terrorism Act, 2002.

(iv) **Issues with Gathering Evidence:** The intangible nature of cyberspace and cybercrime make traditional methods of gathering evidence inadequate. The 'scene of crime' in cyberspace is completely virtual and so is the object of the crime (data / information), Additionally, this type of evidence can be modified very easily. For example, a criminal may set up a program which erases all evidence from the computer if it is accessed by someone other than himself. In this case, mere access to the computer may erase the evidence. Therefore specific rules are required for extraction of evidence and maintaining its' authenticity.

(v) **Anonymity of Netizens:** A cybercriminal can easily guard his identity. A cybercriminal can use fake identities or create identify clones, for example. This makes gathering of evidence difficult.

(vi) **Monitoring of Crime:** The sheer volume of information involved and being processed every second makes monitoring and tracking of crime very difficult. Countries like United States of America, including India, have put in place extensive internet surveillance programmes to deal with this issue. However, such programmes can also be extremely invasive in the personal lives of individuals, raising questions regarding the protection of privacy. For example, India's Central Monitoring System (CMS), described as the Indian version of America's PRISM, is a mass electronic surveillance data mining program which will give India's security agencies and income tax officials centralized access to India's telecommunications network and the ability to listen in on and record mobile, landline and satellite calls and voice over Internet protocol (VoIP), read private emails, SMS and MMS, and track the geographical location of individuals, all in real time. In can also be used to monitor posts shared on social media such as Face back, LinkedIn and Twitter, and to track user' search histories on Google, without any overnight by courts Parliament. The intercepted data may be subject to pattern recognition and other automated tests to detect emotional markers, such as hate, compassion or intent, and different forms of dissent. Telecom operators in India are obligated by law to give access to their networks to every legal enforcement agency.

One of the primary concerns raised by experts is the sheer lack of public information on the project. There is no official word from the government about how government bodies or agencies will use this information; what percentage of population will be under surveillance; etc. There is no legal recourse for a citizen whose personal details are being misused or leaked from the central or regional database. Unlike America's PRISM project under which surveillance orders are approved by courts, CMS does not have any judicial oversight. There is thus need for extensive legislation on surveillance.

(vii) **Evidentiary value of Electronic Information:** The extensive use of 'IT' for communication and documentation raised a new question on the admissibility of electronic evidence. If a person was being stalked online, can copies of e-mails or screenshots of chat room messages by the stalker be admissible as evidence? The pre-amended Indian Evidence Act, 1872 recognised only two types of evidence, documentary evidence (i.e., paper based evidence) and oral evidence (testimonials of witnesses).

(viii) Validity of Online Transactions: Traditional law does not deal with the validity of e-contracts, digital signatures, e-commerce, etc. For example, is a contract entered into through e-mails legally valid? Can be enforced in a court of law?

Thus, the need was felt to promulgate specialized laws to provide for the following:

(i) Setting clear standards of behavior for the use of computer devices;

(ii) Deterring perpetrators and protecting citizens;

(iii) Enabling law enforcement investigations while protecting individual privacy;

(iv) Providing fair and effective criminal justice procedures;

(v) Requiring minimum protection standards in areas such as data handling and retention; and

(vi) Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence.

Evolution of cyber law

Early Cyber Laws: The computer Misuse Act, 1990 of Great Britain

In the case of *R.*v.*Gold & Schifreen* (1988) the defendants had gained unauthorized access to a computer network. The defendants were charged under the Forgery and Counterfeiting Act, 1981 for 'defrauding' by manufacturing a 'false instrument'. It was held by the House of Lords that:

"We have accordingly come to the conclusion that the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants conduct amounted in essence, as already stated, dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."

This judgment brought the possibilities of cyber-crime and the inadequacy of existing laws to deal with them to the notice of the legislature of Great Britain. It led to the enactment of the Computer Misuse Act, 1990. This was among the first cyber laws to be enacted. It recognized the following offences:

(i) Unauthorized access to computer material.

(ii) Unauthorized access with intent to commit or facilitate commission of further offences.

(iii) Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Uniform International Standards for Cyber Law: UNCITRAL Model Law on Electronic Commerce, 1996.

With the globalization of business the international community felt a need for a law which would set uniform standards for electronic commerce. This led to the adoption of the UNCITRAL Model Law on Electronic Commerce by the U.N. General Assembly (the Model Law').

This laid down the fundamental principles of e-commerce law:

(i) **Non-discrimination:** This principle requires the removal of any discrimination between a physical document and an electronic one. It ensures that the document will not be denied its' validity/enforceability solely on the grounds of it being in an electronic form.

For example, Article 5 of the Model Law states that the legality of information shall not be denied merely because it is contained in an electronic document.

(ii) Technological neutrality: This principle mandates that the provisions adopted in a law should be neutral with respect to the technology involved. This ensures that the rapid pace of development of technology does not lead to the law becoming redundant in no time.

For examples, Article 7 of the Model Law which lays down rules regarding a valid signature of an electronic document prescribes a reliable 'method' which is used to indicate that person's approval. Since the method has not been specified, the rule is not restricted to the currently accepted method, which is digital signatures, and the law would continue to apply regardless of any new development.

(iii) Functional equivalence: Terms like 'writing', original', 'signed' etc. are specific to paper based documents. This principle sets out the corresponding criteria for electronic communication.

For examples, the law of evidence generally required that the original document should be presented as evidence. For a paper based document, if would mean a document that was actually issued, or with original signatures, or which is not a photocopy or fax of another document. Article 8 describes an original electronic document to be one where the information if contains is the same as that when it was first generated in its final form.

India's First Cyber Law: The information Technology Act, 2000 This Resolution recommended that. 'all states give favourable consideration is the UNCITRAL. Model law an Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper based forms of communication and strange of information'.

India's First Cyber Law: The Information Technology Act, 2000.

In view of the international recognition of electronic transactions and its' growing use within India, the Indian legislature felt the need for providing a legal framework for e-commerce and digital signatures. It led to the enactment of India's first cyber legislation: the information Technology Act, 2000 (the TT Act').

1. **Objectives of the 'IT Act'**: The preamble to the 'IT Act' states as follows:

'An Act to provide legal recognition for the transactions carried out by means of electronic data interchange and other weans of electronic communication, commonly referred to as 'Electronic Commerce', which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic flings of documents with the Government agencies and further to amend the Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Whereas the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law: -

AND WHERAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to peper-based methods of communication and storage of information.

AND WHERAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government service by means of reliable electronic records, BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

The main objectives of this Act, as laid down in its preamble are the following.

(i) To give effect to the U.N. General Assembly's Resoluiton on the Model Law.

(ii) To provide legal recognition to e-commerce –transactions carried out by means of electronic communication.

(iii) To facilitate electronic filings of documents with government agencies.

(iv) To amend the Indian Penal code, Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891, and the Reserve Bank of India. Act, 1934.

2. Scope of the 'IT Act': The scope of the 'IT Act' is as follows:

(i) To give effect to the U.N. General Assembly's Resolution on the Model Law.

(ii) To recognize filing of forms, issue of licenses, receipt of payment, etc. through electronic means by the government.

(iii) To lay down rules in relation to electronic records- receipt, time of dispatch, etc.

(iv) To provide for a controller of Certifying Authorities in relation to issue of digital signature certificates.

(v) To define offences and prescribes panelist.

(vii) To lay down liability of intermediaries.

(viii) To Prescribe extra territorial jurisdiction for cyber offences.

The provisions of this Act are not applicable to the following instruments.

(i) A negotiable instrument.

(ii) A power – of – attorney

(iii) A trust,

(iv) A will, including any other testamentary disposition.

(v) Any contract for the sale or conveyance of immovable property or any interest in such property, and

(vi) Any such class of documents or transactions as may be notified by the Central Government in the official Gazette.

3. **Legislations Amended by the 'IT Act':** In order to fully achieve the objectives of the 'IT Act', corresponding changes were required in other laws. For instance, the Model Law requires that there should be no discrimination between electronic records and normal documents. This mean that the law of evidence would have be amended to recognize electronic records as admissible evidence. Therefore, the 'IT Act' made amendments to the following Acts:

(i) Indian Penal Code 1860

The definition of the term 'electronic record' was inserted. References to the term 'document' were amended to include reference to 'electronic records'. The Extra- territorial jurisdiction of the IPC was expanded to include all offences targeting computer resource in India. Lastly, sections in relation to a false document were amended to include references to a false electronic record.

(ii) Indian Evidence Act, 1872

The definition of 'evidence' was amended to include electronic records. Some important sections that were inserted are on admissibility of electronic records, proof and verification of digital signatures and presumptions as to electronic evidence.

(iii) Banker's Book Evidence Act, 1891

The definitions of 'bankers books; and certified copies' were amended to include data stored in electronic devices and printouts was also inserted.

(iv) Reserve Bank of India Act, 1934

The powers to make regulations were amended to include regulations on fund transfer through electronic means.

Other International Cyber Laws

1. **UNCITRAL Model Law on Electronic Signature (2001):** Electronic signatures were increasingly being used as a substitute for had written signatures. This law sets out international standards for their use. It lays down the same fundamental principle as the model Law, namely, non-discrimination, technological neutrality and functional equivalence. Its key provisions are:

(i) Criteria establishing equivalence between electronic and hand written signatures.

(ii) Equal treatment of methods of creating electronic signatures.

(iii) Duties and liabilities of the signatory the relying party and the certification service provider.

(iv) Recognition of foreign certificates and electronic signatures.

2. **United Nations Convention on the Use of Electronic Communications in International contracts (New York, 2005):** This convention was made to remove the obstacles faced due to the user of electronic communications in international trade. It makes electronic communications and contracts concluded thereby

equivalent in their legality and enforceability to paper based communications. It's key provisions are:

(i) Place of business and related presumptions.

(ii) Registration of legality of electronic communications and electronic contracts.

(iii) Criteria establishing equivalence between electronic communications / contracts and paper based communications / contracts.

(iv) Time and place of dispatch and receipt of electronic communications.

(v) Effect of error in electronic communications.

JURISDICTION

General concept of sovereignty and jurisdiction

Sovereignty

Under traditional international law, a sovereign, independent state is one which has absolute rights and power with respect to a particular defined territory. The conduct of its internal affairs and of its relations with other states is entirely at its discretion and free from external interference from any other state. It has the exclusive and inalienable right to prescribe and enforce the law applicable to its territory. This traditional concept of sovereignty is now restricted by international law, international relations and international concerns. This has been discussed by Jungle Alvarez in the Corfu Channel Case.

'By sovereignty, we understand the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relations with other states. Sovereignty confers rights upon states and imposes obligations on them….

… This notion has evolved, and we must now adopter a conception of it which will be in harmony with the new conditions of social life. We can no longer regard sovereignty as an absolute and individual right of every state, as used to be done under the old law founded on the individualist regime, according to which state were only bound by the rules which they had accepted. Today owing to social interdependence and to the predominance of the general interest, the states are bound by many rules which have not been ordered by their wall".

Justice Alvarez goes on to enlist the obligations imposed on a state as a consequence of the sovereignty:

(i) Obligation to preserve its territory for fulfillment of its international obligations.

(ii) Obligation to exercise proper vigilance in its territory.

(iii) Obligation to have knowledge of criminal act being conducted on its territory.

(iv) Obligation to take measures to prevent the commission of crime on its territory'.

(v) Obligation to inquire into crimes committed on its territory.

(vi) Obligation to inform concerned states of existence of dangers on its territory.

These obligations imply that a state has to be responsible in its exercise of sovereignty. The earlier notion of absolute and unquestionable freedom over its territory has given way to the notion of responsibility towards the international community. A state is subject not only to the treaties that it is a signatory to but also to international law in general Non-fulfillment of these responsibilities'. Especially where crimes are concerned, can lead or repercussions like withdrawal of international co-operation, and sometimes to interference by the international community.

Jurisdiction

The sovereign state alone enacts the laws applicable and the methods of enforcement in its territory. The State had the exclusive right to prosecute persons for offences committed within its territory. The power to hear and decide a given matter is conferred on a court of law by the state alone. This power is known as jurisdiction.

The definition of jurisdiction under Black's Law Dictionary is:

"The power and authority constitutionally conferred upon (or constitutional recognized as existing in) a court of judge to pronounce the sentence of the law, or to award the remedies provided by law, upon a state of facts, proved or admitted, referred to the tribunal for decision, and authorized by law to be the subject of investigation or action by that tribunal, and in favor of or against persons (or a res) who present themselves, or who are brought, before the court in some manner sanctioned by law as proper and sufficient".

The criteria which establish the jurisdiction of a court to deal with a given matter, as laid down under this definition are:

(i) The power of the court to judge that particular matter must be constitutionally conferred.

(ii) The facts in question must be subject to the tribunal's investigation under law.

(iii) The persons in whose favour/against whom the judgment is passed must be present /brought before the court.

(iv) These persons must be presented brought before the Court in the manner sanctioned.

These criteria imply that legal sanction is the most important aspect of jurisdiction. The first requirement. Therefore, is the prescription of jurisdiction. The prescription of jurisdiction serves the purpose of specifying the matters which are within the limits of a given court. This prevents the chaos which can result from there being no specified forum for any matter. It would mean that every court can hear every matter. Jurisdiction of a court was traditionally decided on two grounds the place where the cause of action arises, or on grounds of territory and the nationality of the parties involved, or no grounds, of nationality.

Principles for prescription of Extra-Territorial Jurisdiciton

Extra-territorial jurisdiction or the extension of jurisdiction of a state beyond its normal territorial boundaries, under modern International Law is prescribe based on the following principles.

1. **Territorial principle:** Jurisdiction under this principle is prescribed on the basis of any events that take place , whether in whole or in part, on the state's territory. This principle applies even with respect to a foreign national present on its territory. When the events take place only in part within the states territory, Jurisdiction may be applied on the basis of either of two principles. The first is the objective principle of territoriality, i.e., where the act commenced within its territory but the effects was felt elsewhere.

2. **Nationality Principle**: Under this principle, jurisdiction is applied to an act of an individual committed outside a state's territory, if the individual is a national of the state. Nationality was defined in the Nottebohm case as:

Determination of whether or not an individual is the national of a state is to be determined by each State as per its own law. The principle of real and effective nationality, as was applied in the Nottebohm case, describes the commonly used criteria by states to determine this, which include the habitual residence of the individual concerned, the centre of his interests, his family use, his participation in public life, attachment shown by him for a given country and inculcated in his children, etc.

3. **Passive personality Principle:** The passive personality principle is when the state exercise jurisdiction over a foreign national on the grounds that he has committed an offence against its own national outside its territory.

4. **Protective principle:** Under this principle, jurisdiction is established by a state where a criminal act abroad is derogatory to the security of the state concerned and / or touches upon its vital interest. It involves an act which

affects the national interests of the state, is committed abroad, and does not involve a national of the state, either, as an offender of victim.

5. **Universality Principle**: Under this principle, jurisdiction is established by any state over any person accused of committing a small number of international crimes, such as piracy, war crimes, such a piracy, war crimes and grave breaches of the Geneva Conventions, regardless of the territory or the nationality of individuals involved. This principle is applied to cases where none of the standard grounds for jurisdiction can be applied, or when none of the standard grounds for jurisdiction can be applied, or when the state within whose territory the crime was committed was unable to prosecute the offenders. This principle is applied with respect to crimes which are so abhorrent that the entire international community feels the need to intervene, like war crimes, crimes against humanity, violation of human rights, slavery, torture, etc.

Jurisdiction in cyberspace

Cyberspace has no geographical boundaries which lends a transnational element to cybercrimes. Traditional national and international law are not designed to adequately deal with such a transnational nature of cybercrimes. A transnational crime is identified with reference to:

(i) Jurisdiction

Where the constituent elements of an offence, i.e., the performance of the offence, the circumstances surrounding the offence, or the results of the offence, either occur is another territory, or produce substantial effects in another territory. This removes the requirement to identify a single location for the cybercrime. This is, however, subject to the establishment of a sufficient connection or a nexus between the constituent elements of the offence and its effects in the state's territory.

(ii) Evidence

Where any part of the offence occurred so as to require investigation in another territory, even though the connection isn't sufficient to establish jurisdiction over the often.

The main issues, therefore, which arise with reference to the jurisdiction for a state over a transnational cyber-crime, are with respect to the following.

(i) Substantive jurisdiction : Over an act that usually occurs only partly if at all, within its national territory, and

(ii) Investigative Jurisdiction: To conduct inquires and investigations on international soil.

The former requires adequate domestic and international law prescribing extra territorial jurisdiction over a cybercrime, and the latter requires international co-operation, in the form of multilateral or bilateral treaties, international conventions and mutual legal assistance agreements.

Personal Jurisdiction under the civil procedure code

The general rule for exercise of personal jurisdiction is laid down under section 20 of the civil procedure code, 1908 (the CPC).

The CPC has laid down various rules based on which the Court which will have jurisdiction over a particular matter will be determined. For instance, a suit with respect to immovable property is to be instituted in the Court within whose territorial jurisdiction the property is situated in whole or in part. The application of this rule is, therefore, restricted to immovable property which is situated within India. For a suit for compensation for wrongs to person / movable property, the Court which will have jurisdiction will be either one of the following within whose territorial jurisdiction, the wrong was done, of where the defendant resides / carries on business / personally works for gain. This rule will be applicable only to situations where the wrong against the person/his movable property was committed within India. Section 20 of CPC. Provides for any situations apart from these that have been specifically provided for, and also situations such as where the parties have agreed to the jurisdiction of a Court in a contract. Therefore, in case which do not involve immovable property within the Court's territorial limits, or a wrong to body / movable property that was committed within the Court's territorial limits, Jurisdiction can nevertheless be exercised on proof of any one of the following factors.

(i) All the defendants reside / carry on a business within the territorial limits of the court's jurisdiction.

(ii) Any of the defendants reside/carry on a business within the territorial limits of the Court's jurisdiction.

(iii) The cause of action arises wholly or partly within the territorial limits of the Court's jurisdiction.

The courts have used this section to exercise personal jurisdiction over entities owning websites that could be accessed within their local jurisdiction, on the grounds that theses websites were 'carrying on business; within the local limits of the Court's jurisdiction.

Jurisdiction under the criminal procedure code

Jurisdiction under the Criminal procedure code. 1973 (the "CrPC) is determined based on the rules for the place of inquiry and trial under chapter XIIl. These rules can be summarized as follows:

(i) An offence shall be inquired into and tried by a Court within whose local jurisdiction the offence is committed.

(ii) Where in respect to an offence:

(a) The place of commission is uncertain (may be any of several local areas)

(b) The place of commission is partly in one local area and partly another.

(c) The offence is a continuing one, and it continue to be committed more than one local area: or

(d) The offence consists of several acts in several local areas:

The offence may be inquired into and tried in a court having Jurisdiction over any of these local areas.

(i) For an act which is an offence on account of an act which is done and a consequence which has ensued inquiry and trial maybe at the Court within whose jurisdiction either the act was done/ the consequence has ensued.

(ii) For an act which is an offence on account of its relation with another offence inquiry and trial may be at the court within whose jurisdiction either of the offences was committed.

(iii) For an offence of murder, dacoit, kidnapping, theft, extortion, robbery, criminal misappropriation, criminal branch of trust or involving stolen property, inquiry and trial may be at the court within whose jurisdiction the offence, was committed, the accused was found, the stolen property was received.

(iv) For an offence that includes cheating and is committed by means of letters/telecommunication messages, inquiry and trial may be done at the court within whose jurisdiction the message were sent/received.

(v) For an offence that was committed on a journey/voyage, the inquiry and trial may be at the court within whose jurisdiction the person/thing against whom the offence was committed passed through during the journey voyage.

Jurisdiction under the IT Act

Jurisdiction under the IT Act is prescriber under sections 1(2) and 75 of the IT Act, which are to be read along with the relevant provisions under the IPC.

1. **Section 1(2) of the IT Act:** Section 1(2) of the IT Act prescribe the jurisdiction under the IT Ac:

'It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

2. **Section 75 of the IT Act:** Section 75 of the IT Act prescribes the extra-territorial jurisdiction over offence or contraventions committed outside of India.

   "(1) Subject to the provisions of sub-section (2) the provisions of the Act shall apply also to any offence or contravèntion committed outside India by any person irrespective of his nationality.

   (2) For the purpose of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."

This section extends the jurisdiction of the IT Act to every person, irrespective of Nationality, who commits an offence on foreign territory using a computer within India.

This section grants 'long arm' jurisdiction to this Act. It extends the jurisdiction of the Act to cover any act by any person which involves a computer situated in India and leads to any offence/contravention outside India. When read with section 4 of the IPC, this section is applicable to any offence which affects a computer located within India. The two most important points to be noted are that this section will apply only if the offence involves a computer system located in India, and that this section is applicable irrespective of the nationality of the person committing the offence.

3. **Section 4 of the IPC:** Section 4 of the IPC prescribes extra-territorial jurisdiction for the code:

   "The provisions of this Code apply also to any offence committed by

   (1) Any citizen of India in any place without and beyond India.

   (2) Any person or any ship or aircraft registered in India wherever it maybe.

   (3) Any person in any place without and beyond India committing offence targeting a computer resource located in India.

   Explanation- In this section:-

(a) The word "offence" includes every act committed outside India. Which if committed in India, would be punishable under this Code.

(b) The expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the information Technology Act, 2000."

This section constitutes the long arm provision of the IPC. Clause (3) was inserted vide the Amendment Act. Under sub-clause (3), the IPC will be applicable to:

(i) Any offence which is punishable under the IPC.

(ii) Which is committed by any person, whether a citizen or non-citizen.

(iii) Which is committed outside Indian territory and

(iv) The offence targets a computer resource which is located in India.

Investigative Jurisdiction with respect to Cybercrime

Given the transnational nature of cybercrime, international cooperation is the foremost requirement for effective investigation and prosecution. An international convention on cybercrime needs to deal with several aspects. Maintenance sovereignty, transnational jurisdiction, transnational investigation, collection of evidence and transnational procedures. The Convention of Cybercrime "Budapest convention was the first international treaty to attempt the establishment of better international cooperation for combating cybercrime. It is the only such multilateral treaty in force. It was adopted in 2001 and has since been ratified by 42 states and signed by another 13 states. Many developing countries including India are not signatories to this treaty.

The main achievement of this treaty since its adoption has been to create a minimum harmonization of cyber laws globally, and so initiate a series of reforms in existing g legislation.

1. **Jurisdiction under the Budapest Convention:** Jurisdiction to try cybercrimes under this convention is laid out under Article 22, The Article establishes the uniform grounds for exercising extraterritorial jurisdiction. Keeping the requirement of state sovereignty and mutual cooperation in mind:-

(i) Jurisdiction can be exercised by a signatory state over an offence that is committed on its territory, or on a ship or aircraft "registered with the state. This clause reflects the application of the territorial principle.

(ii) Jurisdiction can be exercised over an offence committed by a national, either within or outside the territory of the state. This reflects the application of the nationally principle.

(iii) When the state refuses to extradite the individual on grounds of his nationally, due measures are to be taken to exercise jurisdiction over him for the offences committed. This clause indicates the adoption of the principle of out dedere out judicare, which means that a state which refuses to extradite a person is bound to prosecute him for the crime committed.

(iv) The exercise of criminal jurisdiction by the state under its domestic law is not excluded under this convention. This clause indicates and attempt by the convention to provide due respect to municipal law as well.

(v) The Article further takes care to preserve the sovereignty of a state by allowing the states to reserve the application of some of its clauses.

(vi) Finally, the Article emphasizes the need to foster international cooperation, by requiring signatory states with concurrent jurisdiction over an offence to consult each other to resolve the issue.

2. **International Cooperation and Mutual Legal Assistance:** The preamble to the Budapest convention states that an effective fight against cybercrime required increased, rapid and well functioning international co-operation in criminal matters. The fools required to achieve such international cooperation are arrangement facilitate investigation and gathering of evidence, and the necessary arrangements for the international transfer of sentenced persons. These arrangements are usually made either by way of treaties (bilateral or multilateral) or reciprocal promises between states.

Mutual legal assistance treaties (MLATs) are arrangements to facilities investigation and gathering of evidence. The general principles of these arrangements are.

(i) Sufficiency of evidence for the making of a request for mutual assistance, to be determined usually by domestic legislation.

(ii) Requirement of dual criminally, i.e. act based on which mutual assistance is sought to be criminal in both requesting and requested state.

(iii) Option of waiving requirement of dual criminally.

(iv) Limitation of use of information obtained as a result of mutual assistance.

(v) Proscribing grounds of refusal of mutual legal assistance protection national / public interest, consideration of severity of punishment requesting state, political offences, human rights considerations, for example, the grant of a right against self-incrimination.

JURISDICTION WITH RESPECT TO E-COMMERCE- USE OF PERSONAL JURISDICTION TESTS.

A webpage can be accessed by anyone sitting anywhere on the globe and therefore, theoretically, the publisher of the webpage could be sued in any country where it was accessed. While the website may be legal in the original place of publication it may not be so in the country where it was accessed. The exposure to liability on such a global scale can have a chilling effect on the use of the internet. The courts, cognizant of such eventualities, consider whether it has personal jurisdiction over the defendant. To determine whether personal jurisdiction exists or not, the following tests are usually applied.

Traditional Personal Jurisdiction Tests

1. **Long Arm Statute:** 'Long arm statutes' are laws of the state which prescribe grounds for exercising jurisdiction over a non-resident defendant. For example, New York's Civil Practice Law establishes personal jurisdiction over a non-resident on the following grounds.

(i) If he conducts business or enters into contract in the state.

(ii) If he commits a tortuous act within the territory of the state.

(iii) If he commits a tortuous act outside the territory of the state which causes injury to a person within the state.

(iv) If he owns or possesses property within the state.

2. **Test of Minimum Contacts:** The test of Minimum Contacts is the traditional rule for personal jurisdiction established in the United States in the case of international show Co v. State of Washington, office of Unemployment compensation and placement at al. The test lays down that a state court will have personal jurisdiction over a non-resident defendant if it has minimum contacts with the state.

"due process requires only that, in order to subject a defendant to a judgment in process requires only that, in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.

The rules for the application of this test have been developed over various case laws, and a non-resident defendant will have minimum contacts who the state if the state.

(i) Direct contact with the state.

(ii) Purposefully availed himself of the privilege of conducting activities within the Forum State, thus invoking the benefits and protections of its laws, i.e. he deliberately engaged in conduct that created contact with the state.

(iii) Entered into a contract which has substantial connection with the state, such as with a resident of that state.

(iv) Satisfied the Calder effects test which looks at the effects of the out of state conduct in the forum state, or the state where the suite is brought.

(v) Placed his product into the stream of commerce such that it reaches the forum state : or

(vi) An intention to serve residents of the forum state.

3. Effects Test: Under this test, a court can exercise jurisdiction over a party's conduct in another state if the contact in another state if the conduct causes effects in the forum state. This usually involves conduct that is expressly aimed at the forum state.

This test was laid down in the case of Calder v. jones, as a rule for determining minimum contacts with the forum state. Here, a resident of California sued an author for libel with respect to a article that was circular in a magazine in California. Both the author and the editor were residents of Florida. The U.S. Supreme Court found that the defendant knew that the article would have a potentially devastating impact upon the plaintiff, especially since the magazine had its largest circulation in California. Therefore they must reasonably anticipate being hauled into a court there, and were held to be liable for this international and tortuous act.

4. General / Specific Jurisdiction: Presently, personal jurisdiction under the US law is determined based on the fulfillment of one of two tests, which are derived from the rules laid down for the test of minimum Contacts – general or special jurisdiction.

General Jurisdiction exists if the defendant has continuous and systematic contacts with the state. For example, a company that has its headquarters within the state, or a person who is domiciled in the state, will be subject to general Jurisdiction.

Specific jurisdiction exists based on a three part test, as observed by the U.S. Court of Appeals in Cybersell Inc. and Ors.

(i) The defendant has contact with the forum which are related to the cause of the action,

(ii) Those contacts amount to purposeful availment of the privilege of conducting activities within the forum, and

(iii) The exercise of jurisdiction is reasonable.

Tests for personal Jurisdiction in Cyberspace

The established tests for personal jurisdiction, such as the tests of minimum contact, effects test and general and specific jurisdiction test, are applied frequently in determining jurisdiction in cyberspace as well. In order in identify a website over which a court can claim jurisdiction, the first step is to determine if the website is a passive website (based on information model) or an active website (based on business model). Further considerations are the geographical locations of the owner of the website, the user of the website and the web server. Finally, and online contracts having a forum selection clause, or a jurisdiction clause, need to be looked into. For instance, in the Yahoo! Case, Nazi memorabilia, the sale of which is banned in France, was being auctioned on the U.S based Yahoo! Website, which was viewed by some residents of France. In a suit against Yahoo!, the French Court applied the Effects Test saying that the website had targeted the public at large including those in France, and two citizens had suffered as a result.

Forum Selection Clauses: Websites usually protect themselves via terms of service agreements disclaimers and click-trap agreements, of clicking on the 'I Agree / I Accept' button. These form online contracts, which usually contain forum selection clauses. Theses clauses mention the law to be applied in case of a dispute, and which courts will have jurisdiction in case a dispute arises. Forum selection clauses are prima facie considered to be valid, unless the enforcement of the clause would be unreasonable. In the United States, these online contracts are usually held to be enforceable, but the opinion on the enforceability of the forum selection is divided.

1. **Test of Interactivity:** Apart from the standard tests for personal jurisdiction, the US Courts have developed the test of interactive specifically for websites. This test examines the level of interactivity that the website has with its visitors. A website can be of two types active or passive. A passive website is one whose purpose is restricted to providing information. A passive website is usually outside the purview of personal jurisdiction. An interactive website, on the other hand, is one whose purpose is not limited to providing information. It is typically part and parcel of a

business model, such as an e-commerce website. Once the interactivity of the website is established, applicability of personal jurisdiction depends additionally on the fulfillment of the minimum contacts test.

In Cody v. Ward the plaintiff a resident of Connecticut, had purchased stocks pursuant to the advice of the defendant, a resident of California. The defendant had posted information regarding the stocks on an online forum and had communicated with the plaintiff through several e-mails and telephone calls. Though the website itself was passive in nature, the court held that the interaction between plaintiff and defendant was sufficient ground to establish purposeful availment and minimum contact.

2. **Sliding Scale Test:** The 'Sliding Scale' or 'Zippo' Test is the most widely accepted test in the US for the determination of the level of interactivity of a website. In Zippo Mfr.co.v.Zippo Dot Com, Inc, the Court observed that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the internet.

The court established a sliding scale on which the interactivity of the website was to be measured. The court recognized three categories of websites of either ends and at the middle of the scale.

(i) Commercial websites. These are websites which clearly to business over the internet. These provide a definite for personal jurisdiction.

(ii) Passive websites: These are websites that provide information only. Usually, personal jurisdiction does not apply to these websites. If the nature of the transaction between the plaintiff and the defendant fulfils the minimum contact tests then personal jurisdiction with apply despite the website being passive.

(iii) Interactive websites: These are websites that provide information, to which personal jurisdiction may apply depending on the commercial nature of the transaction. Here, also, the minimum contact test needs to be applied. The Court opined.

> "The middle ground is occupied by interactive web sites where a user can exchange information with the hose computer, In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. E.g. Matrix, Inc. v.Cybergold, Inc., 947 F. Supp. 1328 (E.E.Mo.1996).

However, courts have implicitly rejected the Zippo test, criticizing the level of interactivity and commercialism sufficient to justify purposeful availment. Therefore, although courts continue to cite the Zippo case, the sliding scale test articulated in the case is being applied inconsistently in practice.

DIGITAL SIGNATURE AND DIGITAL SIGNATURE CERTIFICATES

NEED FOR AUTHENTICATION OF ELECTRONIC DOCUMENTS

Traditional laws provide criteria for establishing the legality and validity of transactions in their paper based form. For example, a contract is usually formalized by both parties signing the document containing the contract. The signature serves as a method of identification of the parties to the contract, and therefore, it indicates their assent to the term of the contract and makes it legally binding on them. Under the law of evidence, the 'original' document constitutes primary evidence, while a copy of the 'original' document constitutes primary evidence. While a copy of the 'original' document constitutes secondary evidence. The 'originality' of paper based documents is usually established with the presence of original handwritten signatures. Can such a formalized version of a contact be made electronically? How would one identify the parties to such a contract? How does one establish the originally of an electronic document?

Definitions under the IT Act

The method of authentication using digital signatures is prescribed under chapter. It of the IT Act. The relevant definitions under the IT Act with respect to digital signatures are as follows:

Asymmetric Crypto System

The IT Act defines the asymmetric crypto system under section 2(1)(f):

'Asymmetric Crypto system means a system of a secure key pair consisting of a private key for creasing a digital signature and a public key to verify the digital signature.

Key Pair

The IT Act defines a key pair under section 2(1)(x):

"Key pair, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that be public key can verify a digital signature created by the private key.

The public key and the private key as used in the asymmetric crypto system are collectivity known as a key pair.

Private key

The IT Act defines a 'private key' under section 2(1) (zc):

'Private key means the key of a create a digital signature.

The private key is used to create a digital signature, i.e., to affix the digital signature.

Public key

The IT Act defines a 'public key' under section 2 (1) (zd):

"Public key means the key of a key pair used verify a digital signature and issued in the Digital signature certificate."

The public key is used to verify the digital signature.

Digital Signatures

The IT Act define a 'digital signature' under section 2 (1) (p):

'Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3'.

A digital signature is the electronic method prescribed under section 3 of the IT Act used to authenticate electronic records. The method currently prescribes combination of asymmetric crypto system with the 'hash functions' another method of verification, to affix a digital signature. A digital signature would be valid only if it is used by a 'subscriber', i.e., the person holding a valid digital signature certificate..

Digital signature certificate

The IT Act defines a 'digital signature certificate' under section w(1)(q):

'Digital signature Certificate means a digital signature certificate issued under subsection (4) of section 35.

A digital signature certificate (a "DSC")has been defined with reference to section 35 of the IT Act, which gives a "certifying Authority" the power to issue a DSC.

Electronic Signature

The IT Act defines an 'electronic signature' under section 2(1) (ta)

"Electronic Signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."

As per this definition any mode of electronic authentication as prescribed by the Government from time to time will be valid. Digital signatures have been included as a type of electronic signature. Electronic signatures, like digital signatures, are legal only if they are issued under an Electronic Signature Certificate.

Electronic Signature Certificate.

The IT Act defines an 'electronic signature certificate' under section 2(1) (h):

"Electronic Signature Certificate means an Electronic issued by the Certifying issued under section 35 and includes Digital Signature Certificate."

Affixing Electronic Signature.

The IT Act defines an 'electronic signature' under Section 2(1) (d):

"Affixing digital signature with in grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating and electronic record by means of Electronics signature.

Subscriber

The IT Act define's a subscriber under Section 2(1) (ZG):

"Subscriber means a person in whose name the Electronic Signature Certificate.

Authentication of electronic record using digital signatures

Section 3 of the IT Act prescribes a method of affixation of digital signatures that combines tow processes the asymmetric crypto system and the hash function.

Asymmetric Crypto system and Encryption

Asymmetric crypto system consists of a public key and a private key, which together form a key pair. The private key is held by the subscriber, and is used to affix the digital signature on the electronic record. The public key is listed on the DSC and is sent to the person receiving the electronic record for him to verify the digital signature. Once verified, it is proof that the electronic record was sent by the subscriber and no one else.)

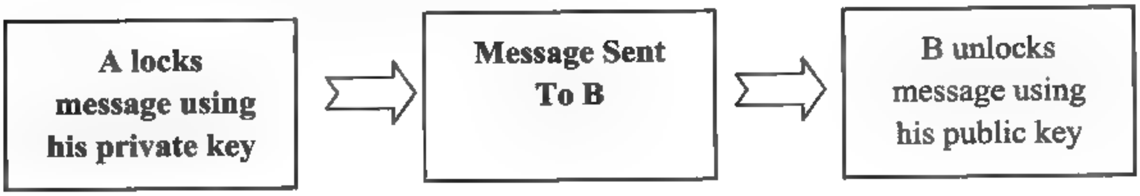
Encryption using a public /private key: The asymmetric crypto user a process known an encryption for the purpose of authentication. It is a process which is used to mathematically encode and decode text in such a way that only intended parties can read it. When, an electronic document is mathematically encoded. Converted into a code, it is said to be encrypted. The coded version of the documents is said to be in the form of cipher text. When this encrypted document is mathematically decoded. i.e. converted into plain text, it is said to be decrypted. The private key is used to encrypt the electronic document, and the public key is used to decrypt it.

The key pair is generated using a cryptographic algorithm, of a mathematical formula, which creates two mathematically related numbers, one of which forms the public key and the other the private key from the public key is mathematically impossible, or computationally infeasible.

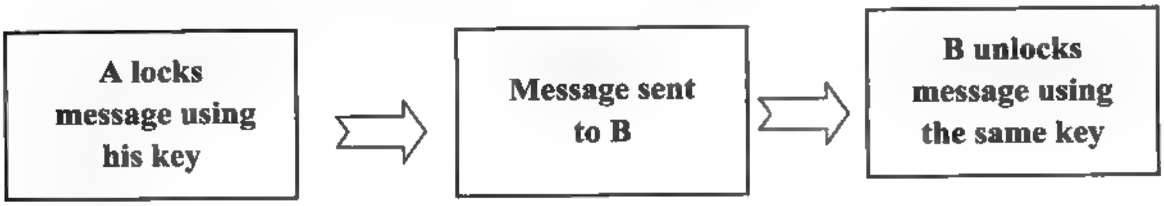
In practice, the encryption can be used in the following ways:

(i) Asymmetric encryption: This is where the sender encrypts his electronic record using the publicly available public key.

For Example, if the sender is A, his private key is A1 and his public key is A2 and the recipient is B. Here, A applies A1 to encrypt the electronic record and sends it is to B. A2 made available to B who uses it to decrypt the electronic record received by him.


A locks message using his private key
Message Sent To B
B unlocks message using his public key

(ii) Symmetric encryption: Here, instead of having one private key known only to the sender and a public key known to the public, there is only one single secret key. This secret key is known to both the sender and recipient, and to no one else. The key is used by the sender to encrypt his electronic record, and the same key is used by the recipient to decrypt the electronic record.


A locks message using his key
Message sent to B
B unlocks message using the same key

In the same example given above, this form of encryption will not involve A's key pair. It will instead involve only one private key, A1. Therefore, A encrypts the electronic record using A1, and sends it to B. B will decrypt the record using the same key. A1, which had been made known to him.

(iii) **Double encryption:** This is the most secure form of encryption. It consists of asymmetric encryption with two sets of keys - the sender's public and private key, and the receiver's public and private key:

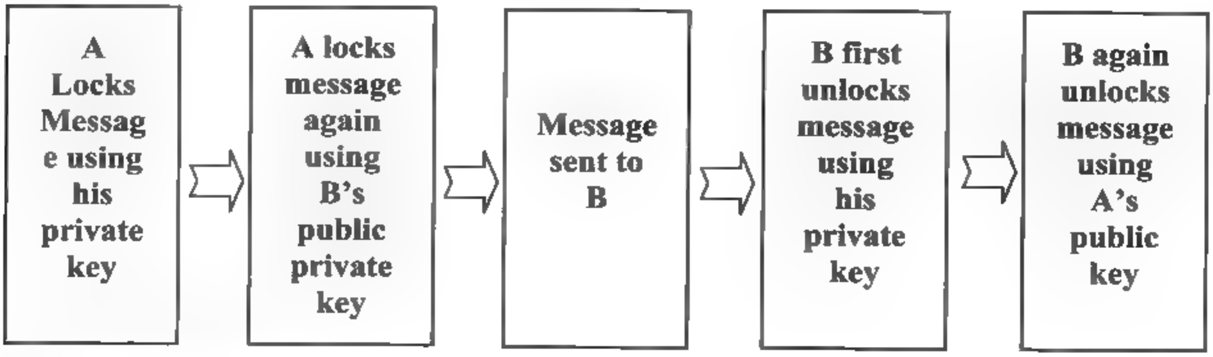
(a) First, the sender encrypts the electronic record using his private key. This ensures that it is the sender himself who is sending the electronic record.

(b) Next, the sender again encrypts this encrypted electronic record using the receiver's public key. This step ensures that no one other than the recipient can access the encrypted electronic record.

(c) On receiving the doubly encrypted electronic record, the receiver first decrypts the electronic record using his own private key. He now know that no one else had access to this electronic record.

(d) Next he again decrypts the electronic record using the sender's public key. The recipient now knows that the sender himself sent this electronic record.

In the example given above, this method of encryption will also involve B's key pair. B1, is private key, and B2, his public key, along with A's key pair. Here, first A applies A1 to encrypt the electronic record. Then he encrypts it again using B2, and sends it to B. B first decrypts the record using B1, and then decrypts it again using A2.


A Locks Message using his private key
A locks message again using B's public private key
Message sent to B
B first unlocks message using his private key
B again unlocks message using A's public key

The Hash Function

Hash functions are used in digital signatures to guarantee the integrity of an electronic record. It has been defined under the explanation to Section 3 of the Act which is as follows:

"Hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as 'Hash Result' such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible.

(a) to drive or reconstruct the original electronic record from the hash result produced b the algorithm:

(b) that two electronic records can produce the same has result using the algorithm.

The hash function uses a method that is very similar to the process of encryption used in the asymmetric crypto system. It consists of a simpler form of encoding and decoding that converts information of one length no information of a smaller length using a mathematical algorithm.

For a given hash function, the smaller length to which the information is to be converted is fixed. This means that, a given 'has function' will always produce a hash result of the same length, regardless of the length of the information to which it is applied. Therefore, the hash function consists of a many: I translation in comparison with encryption, which uses a 1:1 translation. A given electronic record will always produce the same hash result on the application of the same hash function, and no two electronic records will produce the same hash result on the application of the same has function. Even a slight change in the document will produce a completely different hash result. Therefore, the application of a hash function to an electronic record produces a hash result that is completely unique to the record. This guarantees the integrity of the document, since, even the slightest modification to the document can be detected by an application the same has function to the information.

Another important feature of a hash result is that unlike in encryption, a hash result cannot be 'decrypted' to produce the original result. This guarantees the confidentiality of a message that is sent, ensuing that no person who obtains access to the hash result of a document will be able to derive the original information from it.

In summary:

(i) A hash function consists of an algorithm, mapping or translation, i.e., a kind of mathematical formula.

(ii) This mathematical formula converts one sequence of bits, i.e, information of one length into a sequence of a fixed smaller length.

(iii) This smaller sequence is known as a 'hash result;

(iv) A given set of information produces the same result every time the hash function is applied. It is impossible (computationally infeasible) to calculate or derive the original information from its hash result.

It is impossible for two separate electronic records to produce the same hash result using the same hash function.

Use of Asymmetric Crypto System and Hash Function for a Digital signature under the IT Act.

The method of double encryption is a highly secure form of sending information. The only problem is that it is also a highly time consuming process. As a result, the IT Act prescribes a combination of the 'hash function' and asymmetric encryption to be used as a digital signature.

Section 3 of the information Technology Act, 2000 prescribes the following method of authentication used by digital signature.

(1) Subject to the provisions of this section any subscribes the following method of authentication used by Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation –

For the purpose of this sub-section, 'Hash function' means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic records as its input making it computationally infeasible.

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

In order to understand how the asymmetric crypto system and hash function are used to affix a digital signature, reference needs to be made to Rules 3, 4 and 5 of the IT (Certifying Authorities)Rules, 2000)(the "CA Rules)").

1. **Manner of Authentication by a Digital Signature :** Rule 3 of the CA Rules prescribes the manner in which information be authenticated by means of Digital Singarue:

   "A Digital Signature shall,-

   (a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again:

   (b) use what is known as "public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

   Explanation: Computer equipment and software utilizing two such keys are often termed as "asymmetric cryptography".

Under this rule, the affixation of a digital signature involves two steps – creation and verification. This is done using cryptography, which involves the conversion of the message into an unintelligible form and vice-versa. The method of cryptography that is adopted here is 'public key cryptography;, which involves two keys, one which converts the information into an unintelligible form, and the other which reconverts it into the original form. The first key, the private key, creates the digital signature, while the second, the pubic key, verifies it.

The explanation defines 'asymmetric cryptography' to refer to the computer software and equipment which is involved with the use of the public key cryptography.

2. **Creation of Digital Signature :** Ride 4 of the CA Rules describes the process of creation of the digital signature.

3. **Transmission of the Record:** The process of transmission of the electronic record is described in the last part of Rule 4 of the CA Rules. After the digital signature is created, it is attached to the original electronic record. Thereafter, both the original electronic record in plain text and the digital signature are transmitted to the recipient.

4. **Verification of Digital Signature :** Rule 4 of the CA Rules describes the process of verification of a digital signature:

"The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifier shall check-

(i) if the Digital Signature was created using the corresponding private key: and

(ii) if the newly computed hash result matches the original result which was transformed into Digital Signature during the singing process. The verification software confirm the Digital Signature as verified if:-

(a) the singer's private key was used to digitally sign the electronic record, which is known to be the case if the singer's public key used to verify the signature because the singer's public key will verify only a digital Signature created with the singer's private key: and

(b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital signature during the verification process."

Upon receipt of the digital signature and the original record, the recipient will need to verify the digital signature. For this purpose, the public key will have to be made available to the recipient, either, prior to sending the digital signature, or along with the record with the digital signature, or made publicity available for use by any recipient. The Process of verification involves the following steps:

(i) **Creation of a New Hash Result:** The first step in the process of verification is the application of the same hash function to the electronic record received by the recipient. This result in the creation of a new hash result.

(ii) **Application of Public Key:** Thereafter, the public key will be applied to the digital signature that is attached with the electronic record received. This application will decrypt the cipher text, to produce the hash result that was generated by the sender. The successful application of the public key to produce the hash result indicates that the digital signature was indeed created by the application of the sender's corresponding private key.

(iii) **Comparison of the Hash Results:** The next step is the comparison of the hash result obtained by the recipient with the hash result obtained by the sender. Electronic records can very easily be modified or tampered with even once in transit. As mentioned earlier, even a slight change in the document will produce a completely different hash result; change in the document will produce a completely different hash result thus, indicating that the electronic document has been compromised with. On the other hand, the obtaining of a hash function that is identical to the one obtained by the sender indicates that the record received by the recipient was identical to the one that was sent by the sender.

A comparison of the hash result therefore, completes the verification of the digital signature. With this, the process of authentication of the electronic record is complete.

Summary of process of Authentication by a Digital Signature: The steps for the affixation of a digital signature under Section 3 of the Act read with Rules 3, 4 and 5 of the CA Rules can therefore be summarized as follows:

(i) A hash function is applied to the electronic record to produce a hash result.

(ii) The sender's private key is applied to the hash result , to produce an encrypted form of the electronic record. This step indicates the creation of the digital signature.

(iii) This encrypted record is sent along with the original document to the receiver.

(iv) The receiver applies the sender's public key to the document, and decrypts it to obtain the original hash result of the document.

(v) He applies the hash function to the original document sent along with the encrypted record to obtain a hash result again.

(vi) He compares this hash result with the one obtained from the decryption.

(vii) If the hash results are equal, the digital signature is verified.

A digital signature, therefore, guarantees the following with respect to the record:

(i) Authenticity: The asymmetric crypto system guarantees the authenticity of the source of the electronic document, i.e., it guarantees that the document was sent by the sender himself. Since, the private key is known only to the subscriber, the affixation of the digital signature onto the document is evidence that it was affixed by the subscriber and no one else.

(ii) Non-repudiation: The asymmetric crypto system also guarantees non-repudiation of the document , i.e., once the digital signature has been affixed by the sender and verified by the recipient, the sender cannot deny having sent the document.

(iii) Integrity: The hash function guarantees the integrity of the record, i.e., the record had not been altered while being transmitted to the recipient.

AUTHENTICATION USING ELECTRONIC SIGNATURES

Criteria for Valid Electronic Signatures under the Model Law.

Article 7 of the Model Law which lays down the requirement for the functional equivalence of an electronic signature, reads as follows:

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message: and

(b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of the article do not apply to the following: 1.....1"

Thus, the Model law prescribes the following requirements for a valid electronic signature.

(i) It can be used to identify the person.

(ii) It shows the identified person's approval of the content of the message.

(iii) It was as reliable as was required under the circumstances.

Section 3A of the IT Act

Section 3A of the I.T. Act has been enacted keeping in mind these requirements under the Model Law and the need for maintaining technological neutrality.

"(1) Notwithstanding anything contained in section 3,but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic, authentication, technique which

(a) is considered reliable; and

(b) may be specified in the second schedule.

(2) For the purpose of this section any electronic signature or electronic authentication technique shall be consider reliable if.

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person:

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person:

(c) any alternation to the electronic signature made after affixing such signature is detectable.

(d) any alternation to the information made after its authentication by electronic signature is detectable: and

(e) if fulfils such other conditions which may be prescribed.

(3) The central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of parliament.

Instead of specifying the technology to be used for electronic signature, the Legislature specified certain criteria based on which a technology may be prescribed by the Government as a valid electronic signature. An electronic record can be authenticated using any form of electronic signature or other authentication techniques, which is:

(i) Reliable, and

(ii) Specified in the second schedule to the Act.

The second clause specifies when an electronic signature / technique is considered to be reliable:

(i) The data or technology used for the authentication / creation of the signature can be linked to the signatory /authenticator only.

(ii) The data or technology used for the authenticates/creation of the signature was under the control of the signatory/authenticator and no other person.

The process of verification of these signature s and signatory/authenticator may be prescribed by the Central Government.

The prescription of these criteria has given the Government the freedom to keep pace with rapidly evolving technology without needing to amend the IT Act. Clauses (4) and (5) of this section gives the Central Government the power to add/omit signatures/authentication techniques from the second schedule of the Act, provided such signature/authentication techniques meet the requirements specified under this section.

Examples of Electronic Signatures

Currently, there are no electronic signatures prescribed under the second schedule of the IT Act. However, several electronic signatures apart from digital Schedule of the IT Act. However, several electronic signature apart from digital signatures are currently in use:

(i) Click – Wrap Agreements – 'I accept' button on websites.

(ii) PIN Numbers – ATM cards, etc.

(iii) Digitized Image of Hard written Signature

(iv) Biometric Signatures – Electronic devices which scan fingerprints, hand geometry, retina scans, voice recognition, etc.

(v) Signature Capture Devices – Devices such as tablets, signature pads, tc. Which capture handwritten signature.

(vi) Identity Verification Services – E-mail validation, ID verification, etc.

Concept of Secure Electronic Signature

Under Section 15 of the electronic signature is deemed to be securing, if.

(i) The data used to create the signature. i.e., a private key in the case of a digital signature was, at the time of affixing the signature, under the exclusive control of the subscriber only.

(ii) The data used to create the signature was stored and affixed in a prescribed, exclusive manner.

The concepts of secure electronic signature and secure electronic record have been introduced to indicate the requirement of adoption safety practice by the parties involved. This is crucial for the maintenance of the security and integrity of information, especially from the perspective of digital evidence.

Public Key Infrastructure

Public key infrastructure (PKI) refers to the entire organizational structure that is responsible for the establishment and maintenance of a reliable system of public key cryptography

The purpose of the PKI is to generate trust in the electronic environment. In the absence of trust in the security of the transmission and the content of communication, e-commerce and e-government will not find acceptance among parties. The PKI is the medium that establishes the validity and legality of the digital signatures being used by subscribers and of the bodies issuing digital signatures to subscribers. It guarantees the authenticity of the electronic signatures, thereby guaranteeing the enforceability of the electronic transaction for which the signature is used.

The legal basis for the PKI in India is found under Chapter VI[14] of the IT Act, along with various rules issued by the Government, such as the CA Rules and the IT (Certifying Authority) Regulations, 2001. (the hierarchy of the PKI which is established hereby is as follows:

Controller of Certifying Authorities

↓

Certifying Authorities

↓

Subscriber

At the top of the hierarchy is the controller certifying Authorities, which licenses Certifying Authorities, which in turn issue digital signature certificates to subscribes.

Controller of Certifying Authorities: The Controller of Certifying Authorities (the "Controller") is the apex in the PKI hierarchy appointed by the Central Government for the supervision and control of the Certifying Authorities (the "CA"). Is a function include licensing of the CAs, specifying the form and content of an electronic signature and key, laying down applicable standards for CAs, recognition of foreign CAs, etc.

It has been defined under Section 2(1) (m) of the IT Act as follows:

"Controller means the Controller of Certifying Authorities appointed under sub-section (7) of section 17.

The Controller has set up two subsidiary bodies, the Root Certifying Authority of India and the National Repository of Digital Certificates.

1. **The Root Certifying Authority of India:** The 'Root Certifying Authority of India' (the "RCAI") has been established by the controller to perform its function of licensing of CAs. This licensing is done

through the issue of a X.509 certificate, known as Root certificates, which certificate the public keys of the CAs. It is the highest level of certification in India. The license of a CA can be verified by a subscriber through this certificate on the website of the Controller.

The RCAI issues the 'Certification practice Statement' (the "CPS") which is adopted by the Controller, which is defined as follows:

"Certification Practice Statement means a statement issued by a certifying Authority to specify the practices that the certifying Authority employs in issuing Electronic Signature Certificates."

2. **The National Repository of Digital Certificates:** The National Repository of Digital Certificates (the "NRDC") was set up in view of section 20 of the IT Act, which was later omitted by the Amendment Act. This repository contains all the digital signature certificates issued by the RCAI and by licensed CAs. It also maintains the corresponding CRLs issued by them.

The duties of the NRDC are as follows:

(i) Publishing Public Key certificates of licensed CAs.

(ii) Publishing CRLs.

Certifying Authority: A certifying Authority is a body that has been authorized by the Controller to issue an electronic signature certificate to a subscriber. It is defined under section 2(1) (g) of the TT Act as follows:

"Certifying Authority means a person who has been granted a license to issue an Electronic Signature Certificate under section 24".

A CA is authorized by the controller via a 'Root Certificate', as explained above. Thereafter, CA plays two key roles in the PKI system firstly, it issues digital signatures to the subscriber, and secondly, it verities the digital signature of a subscriber on the request of the recipient, or the relying party. In order to perform these roles in a secure manner, the following obligations have been imposed on the CA.

(i) Protection of their private key.

(ii) Maintain a web site and publish the license, sub-CA certificates.

(iii) Publish the name and contact information of the party responsible for the CA.

(iv) In case of a compromise in their signing key, immediately revoke all subscriber certificates, publish details in the CRL and report to the RCAI.

(v) Have their CPS approved by the Controller.

List of Licensed CAs in India: The following organizations have been given a license to operate as CAs in India.

(i) Tata Consultancy Services.

(ii) National Informatics centre.

(iii) iTrust CA, IDRBT

(iv) safescrypt CA services, Sify communications Ltd.

(v) (n) Code Solution CA.

(vi) E-Mudhra

Subscriber: As the bottom of the PKI hierarchy is the subscriber. The subscriber is imposed with the obligations of obtaining a valid DSC from a licensed CA and thereafter, maintaining its authenticity by suitably protecting the private key. A DSC acts as proof linking a particular subscriber to a particular key pair. It contains the following information.

(i) Serial Number (assigning of serial number to the DSC by CA to distinguish it from other certificate):

(ii) Signature Algorithm Identifier (which identifies the algorithm used by CA to sign the DSC);

(iii) Issuer Name (name of the CA who issued the DSC).

(iv) Validity period of the DSC;

(v) Name of the subscriber (whose public key the certificate identifies); and

(vi) Public key information of the subscriber.

Thus, the DSC enables a relying party to identify the subscriber, obtain the public key used by him, and verify the legality of the DSC through the public key of the CA issuing it. The relying party, before relying on the digital signature, should also verify the purpose of the DSC, its validity period, key usage and class. Once verified both the relying party and the subscriber are bound by the electronic transaction.

1. **Procedure for issue of DSCs to a subscriber:** Any person can apply to a CA through its Registration Authority for a DSC. The Registration Authority is the body of the CA which interacts with the subscribers for the provision of CA services. The procedure for the issue of DSCs as prescribed under the IT Act and the CA Rules, and can be collectively summarized as follows:

(i) Application shall be in the application form provided by the CA and accompanied with.

(a) The prescribed fee, as per the class of the application.

(b) A certification practice statement or where there is no such statement, a statement containing such particulars, as specified by regulations.

(ii) DSCs are usually issued with a lifetime of one two years.

(iii) On expiry of a DSC, application may be made for its' re-issue.

(iv) The CA may suspend / revoke the DSC.

(a) On receipt of a request from the subscriber / his agent.

(b) On the death of the subscriber.

(c) He subscriber is firm/a company, on its dissolution of winding up.

(d) A material fact represented in the DSC is false / concealed.

(e) A condition for the issue of the DSC is not satisfied.

(f) There is a compromise in the CAs private key / security system.

(g) There is compromise in the DSC owner's private key.

(h) There is misuse of the DSC.

(v) The CA must publish notices of such suspensions / revocation in the CRIs.

2. Duties of subscribers: The duties of subscribers are covered under chapter VIII of the IT Acts.

(i) Generate Key pair: On acceptance of a DSC, the subscriber shall generate the key pair of which the public key is listed in the DSC.

(ii) Duties: The subscriber shall perform such duties as prescribed with respect to an electronic signature.

(iii) Acceptance of DSC: A subscriber is deemed to have accepted a DSC if be publishes it to one or more persons, or in a repository, or in any other manner.

(iv) Certification of Subscriber: Upon acceptance of a DSC, the subscriber certifies that he holds the corresponding private key, and the representations made to the CA and the information in the DSC are true.

(v) Control of Private Key. The subscriber shall exercise reasonable care to retain control over the private key and prevent its disclosures.

(vi) Compromise of private key: to the event of a compromise of the private key, the subscriber shall inform the CA of the same as soon as possible. Until the CA is informed, the subscriber will continue to be liable for the use of the private key.

****

UNIT-2

ELECTRONIC CONTRACTS

Regulation of E-Contracts

Contracts entered into electronically are referred to as electronic contracts. The Model Law recognizes electronic contracts. This recognition comes in view of the increase in "electronic commerce". Electronic commerce involves the use of alternatives to paper-based methods of communication and storage of information. The importance of electronic commerce lies in its ability to *'improve the efficiency of commercial activities, enhance trade connections and allow new access opportunities for previously remote parties and markets, thusplaying a fundamental role in promoting trade and economic development, both domestically and internationally'* .

Model Law, along with the UN Convention on the Use of Electronic Communications in International Contracts 2005, provide for uniform rules to be adopted by member countries to remove the obstacles and uncertainty created by the use of electronic communications and creation of electronic contracts.

Regulation of E-Contracts in India: E-contracts, like all contracts, are governed by the Indian Contracts Act, 1872 (the "Indian Contract Act"). The IT Act merely recognizes the process of contract formation through electronic means and establishes functional equivalence between e-contracts and paper-based contracts. These provisions in the IT Act were introduced to give effect to the corresponding provisions under the Model Law.

Essentials of a Valid Contract: An e-contract in order to be valid will have to comply with the provisions of the Indian Contract Act and any other law governing the transaction. The essential elements of a valid contract as laid down under the Indian Contract Act is discussed below:

(i) Proper Offer and Acceptance: An offer or proposal[4] refers to the intimation of one person's (the offeror) willingness made to another person (the offeree) to do or abstain from doing something. When theofferee signifies his assent to the offer, the offer is accepted[5].

(ii) Intention to Create Legal Relationships: There must be an intention to create legal obligations between the parties.

(Hi) Lawful Consideration: Consideration refers to any act or abstinence or promise of a party at the desire of the other party. The consideration must be lawful, *i.e.,* it must be of some value in the eyes of the law. An agreement without consideration is void[8].

(iv) Free consent: Two or more persons are said to consent when they agree to the same thing in the same sense. Consent is free if it is not caused by coercion, undue influence, fraud, misrepresentation, and/or mistake. An agreement without free consent is voidable.

(i) *Capacity to Contract:* A person who has attained majority, is of a sound mind and has not been disqualified from contracting under any law is competent to contract. An agreement with a minor is *void ab initio.*

A person of unsound mind is one who is incapable of understanding and forming a rational judgment.

(vi) Lawful Object: The object of the contract must be lawful, *i.e.,* it should not be forbidden by law, defeat the provisions of law, be fraudulent, cause injury to person/ property, be immoral or opposed to public policy. An agreement with an unlawful object will be void.

(vii) Certainty and Possibility of Performance: An agreement, the meaning of which is not capable of being made certain is void. An agreement to do an impossible act is void. An agreement, the performance of which has become impossible, will also be void.

(viii) *Agreements not expressly Declared Void:* The agreement should not have been expressly declared to be void, for example, an agreement in restraint of marriage, an agreement in restraint of trade, *etc.*

Types of E-Contracts

1. **Contracts entered Into through E-mails:** E-contracts may be in the form of a contract that is entered into by way of communication through an electronic medium like e-mails) This involves the discussion of various stages of the formation of the contract such as the communication of an offer, acceptance, *etc.* and other negotiations of the various terms of the contract through the electronic medium. The contract that is entered into is non-instantaneous and negotiable. The Model Law and the IT Act provide the rules applicable to the formation of contracts in this manner.

2. **Standard Form E-Contracts:** Alternatively, e-contracts can take the form of non-negotiable and instantaneous contracts of the following types:

Click-Wrap Agreements*:* This is the most common form of e-contracts found online. It consists of a list of terms and conditions, to which the party can either agree to by clicking on the "I agree' icon, or disagree by clicking the 'Cancel' T Disagree' icon. There is no scope for any negotiation in these contracts. The party only has the option to reject or accept the terms of contract in their entirety. Such agreements have been extensively challenged in the US courts, primarily on the ground that such contracts do not provide adequate notice to the internet user. A few important decisions are discussed:

(i) In *Forrest v. Verizon Communications Inc,* a forum selection clause present in a clickwrap agreement was enforced. It was held that the fact that only a portion of the agreement could be viewed in a scroll box did not imply that the notice to the user was inadequate.

(ii) In *CoStar Realty Info., Inc. v. Field*[21]and *Segal v. Amazon.com, Inc.*, it was held that a click wrap agreement would be binding even if the user had failed to read the contract before accepting it.

(iii) In *Fteja v. Facebook, Inc.*, the terms of service in the form of a hyperlink below the sign up button was held to amount to adequate notice to the user:

Browse-Wrap Agreements: Browse-wrap agreements list out their contract /terms and conditions (usually in the form of a hyperlink at the bottom of the website) on the website being accessed or the product being downloaded. Unlike a clickwrap agreement, where the user must expressly accept the terms and conditions by clicking on an "I agree" box, a browse-wrap agreement does not require this type of express acceptance of the terms. Here, the mere use of the product, for instance, browsing through the website or downloading the product will amount to the user's assent to the contract. The enforceability of these agreements is, however, dependent on whether the user had actual or constructive notice of the terms and conditions;

(i) In *Specht v. Netscape Communciations Corp,* the Second Circuit . Court of Appeals held that a browse wrap agreement which was contained in a hyperlink that could not be viewed unless the user scrolled down to the next screen, did not constitute adequate notice to the user, and the clicking of the download button did not amount to consent to the agreement.

(ii) In *Ticketmaster v. Tickets.com*[25], it was held that knowledge of the defendant ofthe terms and conditions to the website which were contained at the bottom of the home page in small print would have to be proved.

(iii) In *Hubbertv. Dell Corp,* The Illinois Court of Appeal held that the a browse wrap agreement to which the consumers received repeated exposure in the form of the words "All sales are subject to Dell'sTerm[s] and Conditions of Sale" in a series of pages which had to be accessed to complete a purchase, and a conspicuous blue hyperlink to the terms and conditions, was enforceable.

Shrink Wrap Agreements: Shrink wrap agreements were found inside the sealed packaging of tangible products, where one cannot see the agreement until the product has been purchased or used. For example, software CD came packaged in plastic with a notice that by tearing the plastic, the user will be deemed to have assented to the terms of use which are enclosed in the CD. The plastic packaging usually contained some of the essential clauses of the terms of use in brief so as to constitute adequate notice to the user. Such agreements are likely to be found unenforceable on grounds of inadequate notice to the user, unless constructive notice can be established. It is from the term 'shrink wrap' that the terms 'click wrap' and 'browse wrap' have been derived.

Thus, to ensure enforceability of standard form e-contracts, it is essential for websites to provide adequate notice of the contract. A good example of such notice is this caveat provided conspicuously on the first page of the website:

> *"PLEASE READ THIS AGREEMENT CAREFULLY TO ENSURE THAT YOU UNDERSTAND EACH PROVISION. THIS AGREEMENT CONTAINS A MANDATORY INDIVIDUAL ARBITRATION."*

Not only is the notice in large font, and in bold, caps and italics, it also specifically mentions a key provision of the agreement (the mandatory arbitration agreement) so that the user cannot deny notice later in time by saying, for example, that she did not read the agreement in entirety.

Recognition of E-Contracts under IT Act

1. Section 10A: Validity of Contracts Formed Through Electronic

Means: Section 10A of the IT Act provides for the recognition of contracts formed through electronic means:

> *"Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form*

> *or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose."*

Any stage in the formation of the contract, be it a proposal, acceptance or revocation, may be expressed in an electronic form or by means of an electronic record. The section uses the words 'expressed in electronic form or by means of an electronic record'. The section does not specify how this communication reaches the other party, for instance, it does not state that the electronic record is to be transmitted electronically through the means of a computer. Therefore, this section will apply even to cases where an electronic record is transferred manually; say in the form of a magnetic disk which is delivered to the opposite party by courier.

2. **Article 11 of the Model Law:** Section 10A of the IT Act has been drafted along the lines of Articles 11 of the Model Law on the formation and validity of contracts. It provides that:

> ***"(1) In the context of contract formation, unless otherwise*** *agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.*

(2) The provisions of this article do not apply to the following: [...]."

3. No Effect on Law of Contract Formation: (Section 10A of the IT Act provides for a new means of forming contracts, but, does not in any way affect the Indian Contract Act or any other rules of contract formation. The Indian Contract Act in itself does not specify the means by which the communication in the various stages of contract formation should be made, which means that communication may be made through any means which has the effect of communicating the proposal acceptance or revocation. The exception to this rule is when the method of communication is specified, for instance, a specification by the parties to the contract on how the acceptance is to be made. This exception will apply even to cases where the contract is formed through electronic means. Thus, this section cannot be applied to hold a contract as enforceable in cases where a mode of communication other than by electronic means was specified by one of the parties, but, the communication was instead made by the other party through electronic means. Additionally, this section does not affect any other rules that may be applicable for the validity of the contract, for instance, the requirement of notarization.

This is in line with the intention behind Article 11 of the Model Law. With respect to this Article, the Guide to the Model Law that are annexed with the text of the Model Law as to their interpretation stated that the main purpose behind this article was not to interfere with the national law of contract formation, but, instead to settle the prevalent uncertainties in various countries as to the validity of a contract that is concluded through electronic means:

"Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed...

> *... However, the provision is needed in view of the remaining uncertainties in a considerable number of countries as to whether contracts can validly be concluded by electronic means. Such uncertainties may stem from the fact that, in certain cases, the data messages expressing offer and acceptance are generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties. Another reason for such uncertainties is inherent in the mode of communication and results from the absence of a paper document."*

Though, the IT Act is modelled on the Model law, there are many differences in the actual wording of the Act. Therefore, it is to be seen if the Guide to the Model Law will be accepted by the Courts as a guide to the interpretation of the clauses of the IT Act. For instance, the judgments and literature under the UNCITRAL Model Law on International Commercial Arbitration were not accepted by the Supreme Court as a guide to the interpretation of the Arbitration and Conciliation Act, 1996. However, the Guide may still provide direction as to the intent behind and scope of the clauses of the IT Act which are similar to the Model Law.

E-Commerce

E- Commerce is a new way of conducting, managing and executing business transactions using modern information technology.

E-commerce is a 'commerce based on bytes'. E-commerce defined simply is the commercial transaction of services in an electronic format. The World Trade Organization (WTO) ministerial declaration on E-Commerce defines e-commerce as, "the production, distribution, marketing, sales or delivery of goods and services by electronic means." The six main instruments of e-commerce that have been recognized by the WTO are telephone, fax, TV, electronic payment and money transfer systems, EDI (Electronic Data Interchange) and the internet.

The development of e-commerce is like a roller-coaster ride. It is growing but is facing bumps as well. One may say it is part of the growing up process. The first phase of e-commerce threw up a new business nomenclature using various permutation and combination of Business and consumers like Business –to-business (B2B), Business –to- Consumers (B2C), Consumer –to- Business (C2B) and Consumer-to consumer (C2C).

Business –to- business (B2B)

It is a business platform involving two independent or even dependent business entities. It acts a business facilitator, negotiator and dealmaker between or among mutually contributing business units.

Business –to-consumer (B2C)

It refers to a business platform, involving a business entity and consumers. It is a retail version of e-commerce- selling goods or service through web based shops. It is based on the concept of shopping at convenience. A consumer can shop at his convenience from the place and time of his choice. It is about a new shopping experience, through an electronic version of catalogue (mail order) shopping.

Consumer –to- business (C2B)

\it is a kind of retail marketing platform, where a business entity seeks or rather chases customers actively. It is a pro active version of e-commerce in the sense that it is a customer chaser, offering customers deals, packages or bundle of products at competitive prices. Moreover, it negotiates or bids by offering best possible deals to the customers. It is often referred to as reverse auction. These days it is a common business model adopted by airlines and tour operators. This process of reverse auction is resulting into major savings for the manufactures, as suppliers bid for the purchase orders.

Consumer –to- consumer (C2C).

It represents a consumer business platform, where one consumer acts as a resource person selling goods in an online medium to other consumers at a price. One may call such processes as 'consumer 2 consumer auctions '. This is an improvement over traditional selling or auction processes, where the relationship is in the form of 'business 2 consumer'. Another important activity that is generated by such 'consumer 2 consumer' auctions is in the realm of resale and rentals. That is, it has helped in creating a market for second hand goods.

This 'business-consumer' relationship, whether in the form of 'business2business', 'business2consumer', 'consumer2business', 'consumer2consumer', has manifested itself in the electronic marketplace in the form of highly specific business models in Internet space.

Electronic Data Interchange [EDI]

EDI has been accepted universally as a replacement for the traditional paper trading. EDI transactions are also often referred to as the paperless trading. EDI has been defined as 'the computer to computer transmission of business data in a standard form'. According to the United Nations Trading Interchange Directory (UNTID) , Electronic Data Interchange means business communication which replaces paper with high electronic message. It is more secure than simply using e-mail. It may be noted that the Information Technology Act has expressly recognized EDI as a mode of communication. EDI transactions now have legal sanctity in India and it is a foregone conclusion that valid and enforceable contracts can be formed using EDI. However, the inapplicability of the Information Technology Act, to certain types of contracts which are required by existing law to be in writing and which also requires signature makes the applicability of EDI narrow. The exact processes involved in the EDI mechanism are intricate and an elaborate discussion into the field may be beyond the scope of this chapter. In an EDI transaction, the persons entering into such transaction agree on the technology to be used for such communication by way of a separate agreement. Such agreement is referred to as an 'umbrella agreement'.

Online Credit Card Payments

The most dramatic revolution in payment methods in the past few decades has, undoubtedly, been the plastic card. The credit card is the payment vehicle of convenience, which provides its holders with multifarious benefits.

Credit cards in fact are a subset of the general category of payments cards, i.e., cards whose production (whether or not any other action is required) enables the person to whom it is issued (the holder) , to discharge his obligations to a supplier in respect of payments for the acquisition of goods, services, accommodation or facilities, the supplier being reimbursed by a third party, whether or not the issuer of the card, and whether or not a fee is imposed for such reimbursement.

A credit card has been defined as a payment card, the holder of which is permitted under his contract with the issuer of the card to discharge less than the whole of any outstanding balance on his payment card amount on or before the expiry of a specified period, subject to any contractual requirements with respect to minimum or fixed amount of payments. The card permits the holder to obtain credit up to a stated maximum amount from the issuer upon the card's presentation to a merchant. The card issuer sends the cardholder periodic statements (usually monthly) describing the purchase made. The cardholder may settle the indebtedness without interest by paying the entire amount on receipt if the statement or the cardholder may settle the indebtedness by installments, paying interest on the outstanding amount.

Credit cards on the Net

The other area where credit cards will perform a metamorphosed role, is on the internet. It seems natural that online commerce would be done with credit cards. No physical paper needs to be passed unlike cash or checks. We simply type our credit card number into the merchants World Wide web(WWW) page payment form and wait for our purchase to be shipped to us. The only thing that needs to pass between the merchant and the buyer is the credit card number. Of the manifold problems that credit card transactions over the internet have become involved with, possibly the formidable is that of the security. The internet is perceived as a medium in which security and privacy are practically non existent. Therefore, with the possibility of the credit card frauds looming large over them, customers are reluctant to even enter into transactions that could involve the transmission of "sensitive" information over the internet. The consequence of this has been that a number of corporations are engaged in the process of creating a system with some measure of security.

One of the simplest methods in use is simply de-linking the purchase process from internet. Thus once the item is selected over the Net, the credit card number has to be independently delivered through a phone call to the retailer.

The next method that was developed which is currently used by many sites, is hosting the WWW site on a secure server. A secure server is one that uses a protocol such as SSL or S-HTTP to transmit data between the browser and the server. These protocols encrypt the data being transmitted, so when you submit your credit card number through their www form it travels to the server encrypted.

In order to ensure customer trust and still maintain the security of credit card transactions on the net, some companies evolved a systems to cater to the unique nature of the internet. One of these was First Virtual.

The First Virtual system ensures the security of credit card numbers through the use of substitute numbers namely "first virtual personal identification numbers" (PIN numbers). These numbers are of no use, even if intercepted because purchases cannot be charged to them. The first virtual system works by ensuring that a person's account is never charged without e-mail verification from them, whereby the cardholder accepts the charge.

First Virtual uses email to communicate with a buyer to confirm charges against their account. Sellers use either email, Telnet or automated programs that make use of First Virtual's Simple MIME Exchange Protocol (SMXP) to verify accounts and initiate payment transactions.

Cyber Cash

CyberCash operates on a different footing from First Virtual. It simply ensures encrypted passage over the Internet for the credit card data. Moreover, CyberCash requires a special program (Cyber cash Wallet Software program). The user must then register with CyberCash. Registration would include creation of a "wallet ID" and a password. Additionally, one or more credit cards must be attached to the wallet.

Merchants must firstly open an account with an acquiring bank that supports Internet transaction using CyberCash payment systems. They must also install their part of their part of the Cybercash software namely Cybercash Internet Payment Software (SMPS), which will enable communication with both the customers CyberCash wallet, and Cybercash's own servers.

Secure Electronic Transaction. (SET)

SET is a proposed standard for the conduct of credit card transaction over the internet. SET is a set to become the dominant system of paying by a plastic over the net. The aim of SET will be to develop a simple, inexpensive way for the conduct of these transactions, with the maintenance of as much of the same infrastructure as is in use at the moment, thus keeping costs down.

The SET system functions on generally the same pattern as the CyberCash system. Thus there is a need for special SET software, processing is like ordinary cards transactions, etc. However, with SET there will be no active role to be played by one single entity such as CyberCash. Rather, any entity appointed by the Banks or the Banks themselves may perform the function of translating the request format used by acquiring banks.

UNIT -3

Cyber Crime

NATURE AND SCOPE OF CYBER –CRIME

A cyber-crime is any crime committed using a computer. There is no statutory definition of cyber-crime under Indian laws, including under the IT Act. A cyber-crime can be defined as:

> *"Any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime."*

As explained earlier,[a cyber-crime encompasses any crime involving a computer system or network, where such system or network is a target of the crime (for example, hacking), tool of the crime (for example, credit card frauds) or as a repository of evidence related to -the crime (for example, information stored in a computer that aids investigation)] Cyber-crimes include crimes which are specific to computers such as hacking, e-mail spamming and denial of service attacks, as well as conventional crimes committed using a computer, such as theft, fraud and extortion. As a result, a cyber-crime may invite the application of not only the cyber-crime specific legislation, which is the IT Act, but also general criminal legislation, which is the Indian Penal Code1860. Other laws will also be applicable depending on the nature of the crime for example, the Prevention of Money Laundering Act, 2002 will be applicable to a case of online money laundering.

Cyber-crime has a widespread adverse impact, especially in view of the indispensability of the internet in everyday life. The targets of cyber-crime include any device which can access the internet, like a computer, smartphone or laptop, and any activity that is conducted using IT. Cyber-crimes like phishing, spamming, credit card frauds and identity theft now affect between 1-17% of the population, as compared to less than 5% for traditional crimes like burglary, robbery and car theft.

Cyber criminals no longer require an advanced knowledge of computers or a specialized skill set, which means that anyone and everyone can commit a cyber-crime. Apart from isolated individuals committing cybercrimes, the realm of cybercriminals has expanded to include organised and professional hackers and crackers, the 'cyber mafia'[4], and the conduct of cyber war, cyber terrorism and cyber espionage by governments against each other[5]. It is estimated that upto 80% of cyber-crimes today, which are involved in malware creation, botnet management, harvesting of personal and financial data, data sale, etc., are a result of organized activity. The Europol has warned of the huge potential of increase in the volume of organized cyber-crime, especially with respect to the possibility of creation of botnets of mobile phones and the vulnerability of the corporate world due to the number of private devices (individual mobile phones, laptops, etc.) involved.

CYBER CONTRAVENTIONS AND CYBER OFFENCES UNDER THE IT ACT

The IT Act prescribes for both offences and contraventions. A contravention constitutes a violation of a provision of the law which usually results in a suit in a civil court. The contravener is punishable with payment of a penalty to the appropriate authority or damages by way of compensation. An offence, on the other hand, constitutes a more serious violation of the law, or the commission of an act that is prohibited by law, which results in a prosecution in a criminal court. The offender is punishable with payment of a heavy fine, or imprisonment or both. For example, a person who merely accesses a computer without the permission of the owner commits a cyber-contravention. On the other hand, if he accesses the computer with an intention to cause some kind of harm, then, he commits a cyber-offence Accordingly, the punishment will also vary; mere access will lead to the payment of damages by way of compensation, while access with wrongful intent will lead to imprisonment of upto 3 years, or fine of upto Rupees 5 lakhs, or both.

Differences between Cyber Contraventions and Cyber Offences

Differences	Cyber Contraventions	Cyber Offences
Nature of the Crime	Violation of a law or a rule of procedure	Serious violation of law, or commission of act prohibited by law
Sections of the IT Act	Sections 43-45	Sections 65-74
Resultant Proceedings	Civil suit	Criminal prosecution
Judicial Authority	Adjudicating Officer for a claim upto Rupees 5 crore Any competent Court for claims above Rupees 5 crore[12]	Any competent Court
Investigation	The Controller or Officer appointed by the Controller[13]	Police officer not below the rank of Inspector
Applicable Penalty	Penalty upto Rupees 25,000, or damages by way of compensation	Imprisonment upto 7 years and/or fine upto Rupees 10 lakhs; Imprisonment for life for
Compoundability	Compoundable, except in case of a previous conviction for the same contravention[15]	Compoundable/ non-compoundable depending on applicable penalty, previous convictions and nature of

Section 43: Penalty and Compensation for Damage to Computer, Computer System, etc.

Section 43 of the IT Act reads as follows:

"If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,-

a) accesses or secures access to such computer, computer system or computer network[or computer resource];

b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;"

If any person steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

For the purposes of this section:

(i) "Computer Contaminant" means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."

Section 43 of the IT Act, lists out certain acts which when committed without the permission of the owner or the person in-charge of the computer and which amount to a contravention. The lack of authorisation is therefore the primary condition required to establish any contravention under this section. An act which exceeds the permission granted will also amount to contravention. A contravener under this section is liable to pay damages by way of compensation. The IT Act originally provided for an upper limit of Rupees 1 Crore on the amount of damages that could be awarded. However, this upper limit has now been removed by the I.T. (Amendment) Act. 2008 (the 'Amendment Act').The contraventions listed under Section 43 of the IT Act, when committed dishonestly or fraudulently, constitute offences under Section 66 of the IT Act and are punishable with imprisonment and fine.

1. **Section 43 (a): Unauthorised Access: Section 43 (a) of the IT Act reads as follows:**

   "accesses or secures access to such computer, computer system or computer network or computer resource;"

The first requirement of 'unauthorised access' is that the access was made without the permission of the person in charge of the computer. As mentioned earlier, this also includes a case where a person exceeds the permission granted. For example, if a person who is permitted a one-time access to a computer for "a specific purpose instead explores other information stored in the computer, he exceeds the permission granted to him, and is therefore liable for unauthorisedaccess. It is important to establish that the person knows that his access to the S computer is unauthorised. The requirement of a password or any other form of authentication for gaining access can be considered to be an adequate indication of the need for authorization. As a result, attempting to crack the password of a computer indicates knowledge that the access is unauthorised, and amounts to an attempt to gain unauthorised access.

This clause refers to 'access' as well as 'securing access'. 'Access' implies the actual access of a computer by a person, while 'securing access' implies obtaining the means to access a computer. For example, a person who obtains the password of a computer with the intention of accessing the computer at a later point of time has 'secured access' to that computer.

Section 43(a) of the IT Act, acts as a foundation for establishing most of the other cyber-crimes, since, successful access is often the first step for the commission of a crime. For example, crimes like hacking, identity theft, etc., all first require securing access to a computer resource.

'Access': This clause needs to be studied with reference to the definition of "access" under Section 2 (1) (a) of the IT Act:

> *"access with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with thelogical, arithmetical or memory function resources of a computer, computer system or computer network;"*

'Access' constitutes any action which leads to the availability or usage of any of a computer's resources, whether logical, arithmetic or memory. This includes actual physical access by a person physically present, as well as remote access through mediums like the internet and wireless systems.It includes the following:

(i) 'Gaining entry': This implies physically accessing the computer, computer system or computer network. For example, a person who plugs a memory device into a physical terminal of the computer has 'gained entry' into the computer.

(ii) 'Instructing': This implies an instruction or order which is given to the logical, arithmetical or memory function resources of a computer, computer system or computer network. For example, a person typing into the keyboard of a computer is giving instructions to the computer. Similarly, a person operating a computer remotely using remote access software like "Team Viewer" is giving instructions to the computer.

(iii)'Communicating': This implies the sending and receiving of information to and from the accessed computer, computer system or computer network. For example, a person transferring data from the accessed computer to his own computer is 'communicating' with the computer.

2. Section 43 (b): Unauthorised Download/ Copying/ Extraction of Data:

Section 43 (b) of the IT Act reads as follows:

> *"(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.:*

The act of downloading copying or extraction of any data, database or information without the owner's permission constitutes a contravention. For example, this includes the unauthorised copying of information from a computer to a USB-drive, or the unauthorised download of videos from a website such as YouTube.

This clause constitutes the basic law governing data theft. The data stored in a computer may include personal data, financial data, trade secrets, intellectual property, and business methods and so on. Theft of this data can result in crimes like credit card frauds using financial data, extortion using personal data and sale of trade secrets to a business rival. This can lead to immeasurable damage, along with being a severe breach of privacy. In New South Communication Corp v. Universal Telephone Co.[17], an ex-employee of a company who mailed certain confidential financial information of the company, which amounted to a trade secret, to his personal e-mail account, was found guilty of trade secret misappropriation. This unauthorised copying of confidential financial information from the company's computer system clearly attracts the provisions of Section 43(b).

'Data': This clause needs to be studied with reference to the definition of "data" and "computer database" as provided under the IT Act:

Section 2 (1) (o) of the IT Act read as follows:

> *"Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized*

> *manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network., and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."*

Data includes any material that is prepared formally for the purpose of processing by a computer. It may be any form, whether in hard copies or soft copies, and whether stored internally on the computer's memory or in any other storage device. Therefore, this includes information on computer printouts, information stored on CDs, any information stored in a computer's hard disk, etc.

'Computer Database': Section 43, Explanation (ii) of the IT Act read as follows:

> *"Computer Database means a representation of information, knowledge facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;"*

A computer database refers to any material that is prepared formally or is produced by a computer for the purpose of use by a computer. This definition is almost identical to that of data. The material may be in the form of text, images, audio or video.

3. Section 43(c): Introduction of Contaminant/ Virus: Section 43(c) of the IT Act reads as follows:

> *"(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;"*

This clause deals with the introduction of a computer contaminant or virus in a computer without the owner's consent. Introduction of the virus into a computer can be done through innumerable ways, such as, through the download of an infected e-mail attachment or other file from the internet, running of a.CD of installation of software that contains malware or transfer through an infected external device like a pen drive. The introduction may be through direct ('introduces') or indirect means ('causes to be introduced').

'Computer Contaminant' and 'Computer Virus': The explanation to the terms 'contaminant' and 'virus' can be found under the Explanation to Section 43 of the IT Act. Section 43, Explanation (i) of the IT Act reads as follows:

> *"Computer Contaminant means any set of computer instructions that are designed-*

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network."

Section 43, Explanation (iii) of the IT Act reads as follows:

> *"Computer Virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource."*

A contaminant or virus refers to any computer program, data or set of instructions which produce an undesirable effect when executed on a computer. The effect produced can be in any form, such as by denying access to the owner, using a computer s resources (like memory or processing resources) tor other criminal purposes, extracting sensitive and confidential information, corrupting files, causing system crashes, etc. These definitions cover the following types of undesirable effects, and therefore, Section 43(c) of the IT Act will apply to the introduction of a programme that produces any of these effects in a computer:

(i) By a computer contaminant:

(a) Modification, destruction, recording of transmission of data or a programme.

(b) Taking over a computer's normal operation.

(ii) By a virus:

(a) Destruction, damage, degradation or adverse effect produced on the performance of a computer resource.

(b) Attaches itself to another computer resource and operates on the happening of a certain event.

Some examples of viruses and contaminants are:

(i) 'Ransomware 'is a form of malware that prevents access of the computer by the owner, and demands a ransom for its removal.

(ii) 'Spyware' is software that collects information about a person or organization, such as their internet activities, their personal data, passwords, etc. One type of spyware is 'key loggers' which is a programme which records what is typed into a keyboard.

(iii) A 'Trojan horse' is a form of malware that appears to perform an authorised function, but in fact performs unauthorised functions such as data theft and system harm. For example, Rogue-AV is a Trojan horse that claims to remove malware, but in fact installs malware into the computer. This form of malware does no replicate itself.

(iv) A 'Rootkit' is software that gains continued access to a computer by attacking the root or administrator access, and exploits the computer resources and other data stored in it. It is designed in such a way that once infected it can escape detection. An example of this is the Son) Rootkit scandal, where a rootkit to prevent ripping of CDs was introduced into the computers of user who played its CDs. This rootkit unintentionally also created vulnerabilities in the computer which exposed it to exploitation by other malware, leading to the scandal on such illegal copy protection measures.

(v) 'Botnet malware' is any kind of malware that is used to infect and take over a large number of computers for the commission of large scale cyber-crime, such as distributed denial of service attack.

(vi) 'Smartphone Malware' is any malware that can affect a smartphone, For example, 'Antammi' for Android phones is in the form of a Trojan horse; it appears to be a ringtone application, but once installed collects information like contact lists, GPS coordinates, SMS archives, etc.

(vii) 'Industrial Malware' includes malware like 'Duqu' and 'Stuxnet', 'Duqu' is used for industrial espionage,- i.e., it collects information that can be used for attacks of industrial control systems, such as stealing public and private keys. 'Stuxnet' is used for industrial sabotage, i.e., it attacks the PLCs or 'Programmable Logic Controllers' of the industry. PLCs are programs that automate and control industrial processes and machine functions, like control of machinery on factory assembly lines, light fixtures, etc.

The only notable difference between the definitions of a contaminant and a virus is that a contaminant appears to be a type of a virus. A virus includes a set of computer instructions, information, data or programme that adversely affects the performance of the computer. A contaminant has been defined as a set of computer instructions that affects the performance of the computer in the manner specified in the definition. Therefore, a virus is the genus and a contaminant is the species. On applying the definitions of a contaminant and a virus to these examples, it is found that spyware is a contaminant, since it 'transmits data'. "Botnet malware" is also a contaminant, since it 'usurps the normal operation' of the computer. A "Trojan horse" is a virus, since it attaches itself to another computer resource and operates on the happening of a certain event. A Trojan horse may also be a contaminant depending on its form and the actual effect produced by it, for example, if it is in the form of a set of instructions which results in damage to the computer.

4. Section 43(d): Damage to Computer Resource: Section 43(d) of the IT Ad reads as follows:

> *"(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network."*

The term 'damage' has been explained in Explanation (iv) to Section 43 of the IT Act:

> *"Damage means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means."*

This clause will be applicable to the unauthorised action of any person that results in a destruction, alteration, deletion, addition, modification or rearrangement of a computer resource. This damage can be done directly or indirectly. A direct from of damage is if a person modifies a file while working on a computer, while an indirect from of damage is if the person inserts a virus that modifies files on the computer. The term 'destroys' includes actual physical damage done to the tangible components of a computer, for example, when someone actually removes a computers' hard disk and breaks it. On the other hand, the remaining terms 'alters, deletes, adds, modifies or rearranges' indicate damage to the intangible components of the computer, for example, when someone erases a hard drive. Another example of damage is an alteration or rearrangement of the instructions contained in the soft form of a computer programme. The section does not specify whether the damage caused should be temporary or permanent, indicating that it covers both.

An example of a cyber-crime covered under this section is data diddling. In this, a series of inconspicuous manipulations are made to data, which result in a significant gain (usually financial) on the whole. For example, if a bank employee transfers a small amount, such as Rupees 10/- from every account every month, the amount is too insignificant to be noticed by most account holders, while over a period of time, it will result in a large gain to the employee.

5. Section 43(e): Disruption of Computer, etc.: Section 43(e) of the IT Act reads as follows:

> *"(e) disrupts or causes disruption of any computer, computer system or computer network"*

The term 'disruption' has not been defined under the IT Act. It is explained in the Oxford Dictionary to mean any disturbance _or problems which interrupt an 'event, activity or process. Therefore, this clause will cover, any action 'which "creates a disturbance to the normal usage of a computer, computer system or computer network. This includes for example of a disruption caused by a virus which prevents the usage of the internet browser (like Chrome, Firefox, etc.) by showing error messages, corrupting files that, are downloaded, etc. Another example is the disruption caused by a reduction in the speed of computer's operation because it has been made part of a "botnet".

6. Section 43(f): Denial of Access: Section 43(f) of the IT Act reads as follows:

> *"(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means."*

This clause deals with the unauthorised prevention of access to a person who is entitled to access the computer, computer system or computer network. The prevention can be caused through any means and includes both direct and indirect denial of access. It includes physical denial of access, i.e., when a person changes the password of a computer, and virtual denial of access i.e., when a person introduces a virus that affects the BIOS of the computer, therefore, preventing it from starting up. Another example of this is where a person changes the network settings and thereby, blocking a particular computer from the local area network.

7. Section 43(g): Facilitation of Access: Section 43(g) of the IT Act reads as follows:

> *"(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under."*

Any person who provides access to a computer, etc., to a third person will also be liable for the unauthorised access. Whether the person providing access is himself authorised or unauthorised to access the computer is irrelevant, provided that he is providing the access without the permission of the owner of the computer. Additionally, the access provided may be physical or remote.

8. Section 43(h): Unauthorised Availment of Services: Section 43(h) of the IT Act reads as follows:

> *"(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network."*

This clause applies where a person uses services and charges them to another person's account. Acquiring the information required for violation of this clause, such as user IDs, passwords, etc. usually involves other preliminary crimes, such as hacking, phishing[21], installation of spy ware, etc. This is the crime of internet time theft, which occurs when a person uses internet hours which have been paid for by another person. Similarly, this clause applies to crimes involving financial identity theft, like online banking and credit card frauds, where a person makes a purchase using the credit card/ online banking details of another person.

9. Section 43(i): Acts Affecting Information Residing in a Computer Resource: Section 43(i) of the IT Act reads as follows:

> *"(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means."*

This clause penalizes any act which brings about an unauthorised effect on the information residing in a computer resource. There is no specification as to the method by which this effect can be brought about. Therefore, for a cyber-crime, this clause is usually applied in conjunction with the previous clauses depending on how the effect was produced. The effect on the information includes:

(i) its destruction, for example, formatting a CD, which is a computer resource destroys the information stored in it.

(ii) its deletion, for example, erasing a file on the computer.

(iii)its alteration, for example, data diddling results in an alteration of information.

(iv)any act which reduces its value, for example, a person converts a high resolution photograph into a low resolution photograph. This reduces the value of the photograph.

(v) any act which reduces its usefulness, for example, a person introduces a virus, leading to an alteration in the code of a program, because of which the program crashes every time it is run. This affects the utility of the program.

(vi)any act which produces any kind of injurious effect on it, for example, a person brings a magnetic force near a computer's hard drive, causing it to get corrupted. This will affect the hard drive 'injuriously'.

This clause needs to be studied with reference to the definition of 'information' under Section 2 (1) (v) the Act:

> *"Information includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated microfiche."*

10. Section 43(j): Modification, etc. of Computer Source Code: Section 43(j) of the IT Act reads as follows:

> *"(j) steals, conceals destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage."*

The term 'computer source code' has been explained under Explanation (v) of Section 43 of the IT Act:

> "*Computer Source Code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.*"

A computer source code is the basic set of instructions based on which a computer program is run. It forms the very core of the computer program, and reflects the creativity of the developer of the source code in directing the computer to effectively produce the required output. The knowledge of a source code can aid computer programmers in modifying the working of the program. It is, therefore, subject to copyright protection. A source code also forms a very valuable asset for a company, since an efficient source code can provide a high competitive advantage to an industry using it and also to the company developing and licensing the software.

This clause penalizes the theft, concealment, destruction or alteration of a computer source code. The theft, etc. of the source code may be done directly or indirectly, i.e., by the contravener himself, through another person, or any other means. In addition to the requirement to prove lack of authorization, this clause also requires an intention to cause damage'. Thus, this clause does not apply to an accidental alteration, destruction, etc.

Section 43A: Compensation for failure to protect data

Indian companies, particularly in the Business Process Outsourcing sector, handle a lot of information from their customers, employees, and other individuals involved with them. This information includes personal information like addresses and dates of birth, financial information like credit card details, health information, business proposals, and other sensitive data. This information is usually stored electronically, making it highly susceptible to misuse by cybercriminals. The responsibility of maintaining its confidentiality was therefore imposed on the companies storing this information. Section 43A of the IT Act, which was inserted vide the Amendment Act of2008, is the first provision in Indian law which deals with data protection:

> *"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."*

Under this clause, a 'body corporate' will be liable for causing wrongful loss or gain to a person due to the disclosure, in whatever form, of the sensitive personal data in its possession. The disclosure should be as a result of negligence in implementation of suitable security measures in respect of the data. Therefore, a body corporate will not be liable under this clause for a disclosure that occurs despite the implementation of suitable security measures. The body corporate will be required to pay damages by way of compensation to the person to whom wrongful loss is caused. The upper limit of Rupees 5 Crore for the quantum of damages was removed by the Amendment Act of 2008.

1. Body Corporate: Section 43 A, Explanation (i) of the IT Act reads as follows:

> *"body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."*

A 'body corporate' is any company, including a firm, sole proprietorship or any commercial or professional association. This definition implies that Government bodies like the Income Tax Department, Consular Passport & Visa Division, Regional Transport Offices, etc., which are not engaged in commercial or professional services will not be subject to this section. Given the amount of sensitive information collected by these departments, the application of this clause to these bodies as well is crucial for the protection of privacy.

An attempt is being made to provide these safeguards through the Right to Privacy Bill, 2011, which seeks to provide protection to individuals whose privacy is unlawfully violated. It proposes to regulate the collection, maintenance, use and dissemination of the personal information of Indian citizens, and provides for penal action for violation of such rights. This Bill will be applicable to anybody that collects personal information for whatever reason. For example, under the current provisions of the IT Act, internet service providers are mandated to provide information such as communication, real-time interception, etc. for the purposes of investigation and surveillance. Intelligence agencies are not subject to Section 43A of the IT Act. This Bill will impose the necessary restrictions on such collection of information, even if it is by an investigation agency or a government body, such as time restrictions on the period of interception, limitations on when privacy can be infringed and limitations on the kind of information that can be collected.

2. Reasonable Security Practices and Procedures: Section 43A, Explanation (ii) of the IT Act reads as follows:

> *"Reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."*

'Reasonable security practices' are practices and procedures applicable to a body corporate for the protection of sensitive information from any unauthorised access, damage, use, modificalloh7"3iscT6sure or impairment. These practices may either be:

(i) Specified in an agreement between the body corporate and the individual in question, or

(ii) Specified by a law in force, or

(iii)In the absence of both of the above, prescribed by the Central Government.

In view of this, the Central Government has issued the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the "Reasonable Security Practices Rules") under Section 43A of the Act to prescribe the required parameters for 'reasonable security practices' and 'sensitive personal data'. Some important provisions under these Rules are:

(i) A body corporate is required to provide policies for privacy and for disclosure of information.

(ii) A body corporate must obtain the consent of the user before collecting information.

(iii) Prior permission must be acquired before a disclosure of personal sensitive information is made.

(iv) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one of the recommended standards for reasonable security practices to be adopted by the body corporate.

2. **Sensitive Personal Data or Information:** Section43A of the Act, Explanation (iii) reads as follows:

> *"Sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."*

Sensitive personal data or information refers to the information that is prescribed as such by the Central Government. The Central Government has prescribed the following parameters for sensitive personal data or information under Rule 3 of the Reasonable Security Practices Rules:

"Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act,2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for eh purpose of these rules.

Section 44: Penalty for failure to furnish information, return, etc. Section 44 of the IT Act reads as follows:

"If any person who is required under this Act or any rules or regulations made there under to:

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the tune specified therefore in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues."

In this section, the following penalty will be applicable to any person who fails to fulfill a requirement under the IT Act or any Rules there under:

(i) Failure to provide any document to the Controller or Certifying Authority, such as the requirement of a Certifying Authority to submit its IT and Security Policy to the Controller prior to commencement of operation.

(ii) Failure to file a return or provide any information within the time period specified, such as the requirement of a Certifying Authority to submit a copy of an audit report to the Controller within 4 weeks of completion of the audit.

(iii) Failure to maintain books of account or records, such as the requirement of a Certifying Authority to maintain the accounts as specified by the Controller.

Section 45- Residuary Penalty

Section 45 of the IT Act reads as follows:

"Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty- five thousand rupees."

"Who ever knowingly or intentionally conceals, destroys or alters or :intentionally "or knowingly causes another' to conceal, destroy or alter any computer source code used for a computer, computer programme computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

> *Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form."*

This section criminalizes the direct or indirect concealment, destruction or alteration of a computer source code. The act must be done either knowingly or intentionally. This is punishable with imprisonment of upto 3 years, a fine of upto Rupees 2,00,000/- or both.

Form of Source Code: A computer source code, as explained above, is the basic set of instructions forming the core of a programme. This section does not specify the language of the source code. Generally, a source code is written in programming .language, i.e., a language that can be read and understood by a programmer. A compiler/ assembler convert this source code into machine language, i.e., the language which is understood by the computer and based on which the computer executes the program. The source code in machine language is known as an 'object code'. Software that is purchased or installed usually comes in the object code. The Act, in its explanation has not differentiated between the two forms, which mean that the section will be applicable to tampering with either the source code or the object code. Further, this section will be applicable to a source code regardless of whether it is in an electronic form, or in a physical form such as in a printout.

Required to be Kept or Maintained by Law': A key factor for the applicability of this section is that the source code was required to be kept or maintained by law. The implication of this phrase was discussed by the High Court of Andhra Pradesh in the case of Syed Asifuddin Case. Here, it was argued that there was no law for the time being in force that required a computer source code to be maintained, and therefore an offence under Section 65 of the Act could not be made out.

Here, the Court rejected this argument, holding that Section 65 of the Act outlined two separate situations, one where a computer source code was required to be kept, and the other where a law required it to be maintained. The Court found that the former situation was applicable to this case, but, whether or not the source code was in fact maintained by the cell phone operator was a matter of evidence:

> *"The submission that as there is no law which requires a computer source code to be maintained, an offence cannot be made out, is devoid of any merit. The disjunctive word "or" is used by the Legislature between the phrases "when the computer source code is required to be kept" and the other phrase "maintained by law for the time being in force" and, therefore, both the situations are different.*
>
> *This Court, however, hastens to add that whether a cell phone operator is maintaining computer source code, is a matter of evidence. So far as this question is concerned, going by the allegations in the complaint, it becomes clear that the second respondent is in fact maintaining the* computer source code."

Difference between 43(j) and 65 of the IT Act: Any act affecting a computer Source code will now attract any one of Section 43(j) and Section 43(j) read with Section 66 and Section 65 of the Act. The main differences between Section 43(j)(Contravention of modification, etc. of source code) of this Act and Section 65(Offence of tampering with a source code), and Section 43(j) read with Section66 (Computer Related Offences) of the Act are:

Basis of Difference	Section 43(j)	Section 43(j) read with Section	Section 65
Nature of Crime	Contravention	Offence	Offence
Effect on Source Code	Deals with theft/ destruction/ concealment/ alteration	Deals with theft/ destruction/ concealment/ alteration	Deals with destruction/ concealment/ alteration
Type of Source Code	Any source code	Any source code	A source code that is required to be kept/ maintained by law in force
Type of Device	Any source code used for a computer resource	Any source code used for a computer resource	Any source code used for a computer, computer system, or computer network
Mens Rea	Intention to cause damage	Fraudulently/ dishonestly + Intention to cause damage	Intentionally/ knowingly
Penalty	Damages by way of compensation	Imprisonment upto 3 years and/or fine upto Rupees 5 lakhs	Imprisonment upto 3 years and/ or fine upto Rupees 2 lakhs

Section 66: Computer Related Offences

Section 66 of the IT Act reads as follows:

> *"If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*
>
> Explanation: For the purpose of this section,-
>
> (a) the word "dishonestly" shall have the meaning assigned to it in section24of the Indian Penal Code;

(b) the word "fraudulently" shall have the meaning assigned to it in section25of the Indian Penal Code."

This section criminalizes the cyber contraventions under Section 43 of the Act when they are committed with a criminal intent) i.e., when they are committed dishonestly or fraudulently. Section 43 of the Act only requires that the act be done without the required authorization and without specifying the mensrea.

Therefore, the two ingredients for an offence under this section read with Section 43 of the Act are:

(i) The act should be unauthorised.
(ii) It should be committed dishonestly or fraudulently.

The penalty applicable will be imprisonment upto 3 years or a fine upto Rupees 5,00,000 or both.

"Dishonestly": The terms 'dishonestly' and 'fraudulently' have been explained to have the same meaning as that under the IPC. The term 'dishonestly' has been defined under Section 24i)f the IPC as follows:

> *"Dishonestly- Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly ".*

For the meanings of the terms 'wrongful gain and 'wrongful loss', reference can be made to Section 23 of the IPC:

"Wrongful gain.- 'Wrongful gain' is gain by unlawful means of property to which the person gaining is not legally entitled."

"Wrongful loss. - 'Wrongful loss' is the loss by unlawful means of property to which the person losing it is legally entitled. -Gaining wrongfully, losing wrongfully.-A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrong-fully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property."

A person is said to have a 'dishonest' intention when he acts with an intention to either unlawfully obtain the property of another, or unlawfully deprive another of his property. The main object behind a 'dishonest' intention is to gain some kind of economic or pecuniary benefit, or cause an economic or pecuniary loss to another. For example, if a former employee steals a crucial source code from his company and sells the code to a business rival, then, he is making a wrongful gain, and if he instead simply conceals the source code, then, he is not making a wrongful gain, but, is causing wrongful loss to the company.

"Fraudulently": The term 'fraudulently' has been defined under Section 25 of the I.P.C. as follows:

> *"Fraudulently - A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise."*

A person with a 'fraudulent' intention, on the other hand, is one with an intention to defraud. An intention to defraud implies the presence of an element of deceit or trickery, and the resultant injury involves both economic and non-economic injury, such as damage to person, body or mind[39]. For example, a business rival poses as an employee and extracts some confidential and defamatory information about a company, and thereafter threatens the company with publication. This involves an element of 'deceit', and the threat can cause economic injury through the extortion and can potentially cause non-economic injury through damage to the company's reputation.

Hacking prior to Amendment of Section 66 of the Act: Prior to amendment, Section 66 of the Act dealt with 'Hacking with computer system', and read as follows:

"(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

'Hacking', being a colloquial term subject to change, was removed from by the Amendment Act, and the section was made all encompassing to cover any offence related to a computer. Hacking was covered in principle under the newly introduced Section 43(i) of the Act. This amendment was, however, widely criticized[41] on the grounds that it greatly narrowed the scope of application of the section, making it difficult for law enforcement agencies to book offenders. The earlier definition of 'hacking' was of very wide scope, covering most computer related offences, and was broad enough to include newly emerging cyber-crimes as well.

The main reason for this criticism was the requirement of the act being conducted 'dishonestly/ fraudulently' under the current Section 66 of the Act. This means that a person is liable for an offence under this section only if the act was committed with an intention to defraud, or with the intention of causing wrongful loss, or wrongful gain. This implies a much higher level of mens rea than in the old Section 66 of the Act, where a person who even had mere knowledge of the likelihood of injury could be held liable. For example, suppose a software consultant hired to install certain software, proceeds with the installation without reading the instructions. Upon installation, the computer automatically reboots, as a result of which the owner loses vital unsaved data. Under the old section on hacking, since, the level of his expertise implies that he had knowledge of the likelihood of injury, he could have been held liable for the negligent 'destruction of information residing in the computer resource'. Since this loss was not caused dishonestly or fraudulently, there will be no remedy under the current Section 66[42] of the Act.

Section 66A: Punishment for sending offensive messages through communication service, etc.

Section 66A reads as follows:

"Any person who sends, by means of a computer resource or a communication device-

(a) any information that is grossly offensive or has menacing character or

(b) any information which he knows to be false, but for the purpose of causing annoyance inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annnoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such message.

Shall be punishable with imprisonment for a term which may extend to three years and with fine."

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

This section applies to the use of a computer resource or communication device for sending messages which are:

(i) Grossly offensive or have menacing character, or

(ii) False, and are sent repeatedly for causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimation, enmity, hatred or ill will, or

(iii) E-mails or electronic message (SMSs) sent for causing annoyance or inconvenience, on with an intent to deceive or mislead.

The message may be in any form so long as it involves a computer resource or a communication device. It may therefore be in the form of e-mails, SMSs, blogs tweets, images, Voice over IP, Skype, etc.

Clause (a) says,

"any information that is grossly offensive or has menacing character".

The first clause of this section deals with the sending of information that is 'grossly offensive' or which has menacing character'. Examples of cyber-crimes to which this clause would apply are cases of online defamation, text bullying online stalking, transmission of morphed/ obscene images, etc.

"Both these terms, 'menacing' and 'grossly offensive' are undefined in the II Act. Some guidance may be drawn from the similarity of Section 66A to Section 127 of the Communications Act, 2003, of the U.K., which deals with the improper use of public electronic communications network:

"(1) A person is guilty of an offence if he:

(a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

(b) causes any such message or matter to be so sent.

(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—

(a) sends by means of a public electronic communications network, a message that he knows to be false,

(b) causes such a message to be sent; or

(c) persistently makes use of a public electronic communications network.

(3) A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.

(4) Subsections (1) and (2) do not apply to anything done in the course of providing a programme service (with in the meaning of the Broadcasting Act 1990 (c. 42))."

On 'Grossly offensive': The meaning of the term 'grossly offensive 'as used in this section was discussed in the case of by the House of the Lords. It was (explained to mean something more than a message that was merely offensive as considered by a reasonable man. What is 'grossly offensive' is to be determined by the Judges] having due regard to the context, surrounding circumstances and the notions of society in general

> *"...it is for the Justices to determine as a question of fact whether a message is grossly offensive, that in making this determination the Justices must apply the standards of an open and just multi-racial society, and that the words must be judged taking account of their context and all relevant circumstances.*
>
> *...Usages and sensitivities may change over time. Language perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates."*

(ii) On 'Menacing': Messages which were 'menacing' in nature under this section were discussed by the U.K. High Court in Director of Public Prosecutions v. Collins[44]to be messages that sought to instill fear in the recipient:

> "A menacing message, fairly plainly, is a message which conveys a Threat - in other words, which seeks to create a fear in or through the recipient that something unpleasant is going to happen. Here the intended or likely effect on the recipient must ordinarily be a central factor in deciding whether the charge is made out."

Clause (b) says,

> "any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device."

This clause applies to the repeated sending of false messages for the purpose of causing inconvenience, etc. as listed therein! This applies to cyber-crimes such as online intimidation, net extortion, online insult, hate mails, cyber stalking and extortion through morphed images. An explanation for the terms used in this clause can be found with reference to similar sections under the IPC, for example:

(i) 'Annoyance', 'inconvenience', and 'obstruction' can be found under the concept of 'public nuisance' under the Section 268 of the IPC.

(ii) 'Danger' has not been defined under the IPC, but has been used certain sections such as Section 336 of the IPC, which deals with an act endangering life or personal safety of others.

(iii) 'Insult' is covered under Section 504 of the IPC, with reference to an intentional insult with intent. To provoke a breach of peace. Insult in general refers to any expression, statement, etc. that is considered derogatory, offensive or impolite.

(iv) 'Injury' is defined under Section 44 of the IPC as any harm cause illegally to a person's body, mind or reputation.

(v) 'Criminal intimidation' is defined under Section 503 of the I. P.C. as a threat to injure a persons' body, reputation or property made with the intention of causing alarm/ causing the person to perform some act.

(vi) 'Enmity, hatred and ill-will' are covered under Section 505 (2) of the IPC, with reference to creating or promoting enmity, hatred or if will between classes.

Clause (c) says,

"any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to

deceive or to mislead the addressee or recipient about the origin of such messages."

This clause deals with two types of mails:

Mails or messages sent with the purpose of causing annoyance or inconvenience, or

(ii) Mails or messages sent with the purpose of deceiving or misleading the recipient as to the origin of such mails.

This clause was inserted specifically for the purpose of dealing with spam and unsolicited mails. It will also be applicable to cases of e-mail spoofing and phishing, i.e., e-mails which imitate mails from financial institutions such as banks and credit card companies in an attempt to extract confidential or financial information from the recipient.

Unconstitutionality of Section 66A of the Act: Section 66A since its introduction into the IT Act has been challenged as being violative of Article 19 (1) (a), or the Right to Freedom of Speech. The main cause of this is the broad phrasing of the section and the lack of any guidance as to their interpretation which can bring any statement which a person may find annoying, insulting, inconvenient, etc. within the purview of the section. These terms are subject to wide interpretation that varies greatly based on the perceptions of people, such as the people writing a message, people reading and people affected by it. This is quite evident in the case of the arrest of two women under this section for posting comments on Face book on Bal Thackeray's death. Comments and personal opinions such as these on blogs, Twitter, Face book and other such sites are very common and in the absence of any parameters to define when taking action under this section is justified, the opportunities of abuse of this section is very high. A higher degree of harm to the people affected by such comments should be required in order to prevent the violation of the right to freedom of speech and maintain the constitutionality of Section 66A. The Government has taken one step in terms of an advisory [2] on the implementation of Section 66A, wherein, it has advised to State Governments (to not allow arrests under Section 66 A without the prior approval of a superior officer. The relevant part of the advisory is as follows:

> *"State Governments are advised that as regard to arrest of any person in complaint registered under Section 66A of the Information Technology Act, 2000, the concerned police officer of a police station under the State's jurisdiction may not arrest any person until he/ she has obtained prior approval of such arrest, from an officer, not below the rank of the Inspector General of Police in the metropolitan cities or of an officer not below the rank of Deputy Commissioner of Police or" Superintendent of Police at the district level as the case maybe".*

Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device

Section 66B of the Act reads as follows:

> "Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same-to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both ".

This section would be applicable to people buying or retaining stolen computer resource or communication device. This includes devices such as, laptops, computers and mobile phones and also other computer resources such as stolen data and software. In the example of a former employee selling a crucial source code to a business rival, the former employee will be liable under Section 43 (i) read with Section 66 (stealing source code with dishonest intent) of the Act, while the business rival, if he was aware that the source code was stolen, will be liable under this Section.

66C: Punishment for identity theft

Section 66C of the Act reads as follows:

> *"Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend for three years and shall also be liable to fine which may extend to one lakh rupees.*

This section applies to any case of cheating by personation which is done using a computer resource or a communication device. The terms 'cheating' and 'cheating by personation' can be better understood on comparison with the corresponding sections under the IPC.

Cheating by Personation: The term 'cheating by personation' has been defined under Section 416 of the IPC as:

> *"A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for*

another, or representing that he or any other person is a person other than he or such other person really is.

Explanation: The offence is committed whether the individual personated is a real or imaginary person.

Illustration:

(a) 'A' cheats by pretending to be a certain rich banker of the same name. 'A' cheats by personation.

(b) 'A' cheats by pretending to be 'B', a person who is deceased. 'A' cheats by personation."

Cheating by personation therefore refers to the act of a person who pretends to be another person, and thereby deceives another person into performing some act. The personation may be of a real individual or an imaginary one.

Cheating: The term' cheating' is defined under Section 415 of the IPC as:

"Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation: A dishonest concealment of facts is a deception within the meaning of this section."

The crime of cheating, defined under Section 415 of the IPC, requires the deception of a person which results in one of the following:

(i) *Inducement to deliver property*: The first part-of the section refers to a fraudulent or dishonest inducement of the person to deliver any property, or consent to the retention of any property.

For example, a person sends an e-mail to a company pretending to be the Director of a reputed company. He induces the other company to enter into contracts with him. On the basis of these contracts, the company sends raw materials to the address given by the impersonator. Section 66D of the IT Act will be applicable to this because of the use of a computer resource, the computer sending the e-mail, in the commission of the offence.

With reference to the IT Act, it can be assumed that inducement or retention of intangible property such as data or information also amounts to cheating. Therefore, in the same example above," if the person induces the company into sharing confident al business information with him, it will still amount to fraudulent inducement to deliver property.

(ii) Inducement to Act/ Omission Resulting in Harm: The second part of the section refers to an intentional inducement of the person to do something which he would not do without the deception, or not do something, which he would normally do where such act/ omission results in harm to his body, mind, reputation or property.

For example, a person posing as a qualified doctor on a website gives some advice to another person for an illness, based on which such person does not take the advice of a real doctor:"As a result, the illness gets worse. This is an example of an intentional inducement to perform an act, which such person would not perform in the absence of the deception, which results in harm to the person's body. Section 66D of the IT Act will apply to this situation as well.

Difference between "Identity Theft" and "Cheating by Personation": The differences between these two offences are:

(i) Identity theft refers to the theft of an actual person's identity, while cheating by personation may be of a real person or an imaginary person.

(ii) Identity theft specifically requires the use of a unique identifier, while the means of personation has not been specified for the offence of cheating by personation. Therefore the personation may be done using an identifier or through any other means.

Section 66E- Violation of Privacy

Section 66E of the IT Act reads as follows:

"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."

Explanation: For the purposes of this section:

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy "means circumstances in which a person can have a reasonable expectation that:

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

> *(ii)* any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place."

This section applies to the violation of the bodily privacy of any person, Capture, publication and transmission refer to three different stages in the violation of bodily privacy. This section criminalizes any of these stages that are done without the victim's consent.

Capture: As explained in the section, capturing refers to capturing an image by any means, such as videotaping, photographing, filming or recording. It may involve any kind of technology, such as video recorders, cameras, CCTVs and other forms of electronic surveillance, spy cameras and other hidden cameras, smartphones, and also the newly developed Google Glass. It also includes situations where the webcam in a PC or a laptop is taken over by a virus and is used to record such images. It can be assumed from the explanation of the term 'capture' that it does not refer to a permanent capture alone. For example, if the webcam taken over by a virus is used to view such images, and not record/ store them, it may still amount to an offence under this section.

It is also essential that the capture takes place under 'circumstances violating privacy', i.e., under circumstances where a person would normally expect to have privacy, such as washrooms, changing rooms, hotel rooms and bedrooms. This includes such circumstances in both public and private places. This section also imposes a restriction on measures in the name of surveillance and security, whether taken by a private party or the Government, for example, installation of a CCTV camera in an office's washroom in the name of security, or a sting operation which results in the capturing of such images.

Publications: Publication, Is explained in the section prefers to i) the creation of copies of the image, whether in physical or virtual form, and if) the making of such copies accessible to the public. Therefore, publication includes publication both in print such as magazines, books or newspapers, and electronic form, such as on websites and CDs. The phrase 'making it available' indicates that it does not matter that the images should have actually been accessed by the public, so long as it is intended for the public to access the image. For example, if such an image was published in a magazine, the section would be attracted regardless of whether or not the magazine was actually purchased or viewed by a member of the public, such as, if the magazines were seized before their distribution. Also, the publication must be done without consent, for example, if such an image was captured with the victim's consent, but, printed in the magazine without consent, the section would still be applicable regardless of the consent to the initial capturing of the image.

Transmission: Transmission refers to an intentional, i.e., deliberate electronic transfer of the image so that it can be viewed by other persons. It includes a transfer to even one other person. Therefore, this would include transfer via e-mails, the internet, instant messaging, bluetooth, etc. Here again the actual viewing of such an image by the persons to whom it is sent is irrelevant, so long as it was sent with the intention that it be viewed by them.

Applicability of Section 354C of the IPC: An offence under this section would also attract Section 354C of the IPC. This section, which was introduced by the Criminal Law (Amendment) Ordinance, 2013, deals with violation of a woman's privacy:

> *"Whoever watches, or captures the image of, a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year. but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.*

Explanation 1- For the purposes of this section, "private act" includes an act carried out in a place which, in the circumstances, would reasonably be expected to provide privacy, and where the victim's genitals, buttocks or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the person is doing a sexual act that is not of a kind ordinarily done in public.

Explanation 2. -Where the victim consents to the capture of images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section."

Cyber Terrorism

Introduction to Cyber Terrorism: Cyber terrorism, as the name indicates, is the use of computers and IT to cause large-scale disruption or widespread fear. The main targets of these attacks are computer operated infrastructure and other facilities that are critical in nature, such as that of e-government systems, financial institutions, military installations, power plants, air traffic control and water systems^: has been explained as follows:

> *"Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*

Forms of Cyber terrorism: Cyber terrorism can take many forms, and the increasing use of IT means that anything can be its target. Some of these possibilities of cyber terrorism and their impact have been outlined below[56]:

(i) Targeted scanning, probing and reconnaissance of networks and IT infrastructure, which can be a pre-cursor to hacking and focused attacks and total or partial disruption of e-governance, public and banking services.

(ii) Large scale defacement and semantic attacks on websites, which can lead to national embarrassment, total or partial disruption of services, dissemination of false or misleading information, etc.

(iii) Malicious code attacks, like virus, worms, trojans and botnets, which can target large and key national and economic databases like tax information networks, citizen databases or hospital information systems, and control systems of sectors like power, petroleum, transport and air.

(iv) Large scale SPAM attacks which can target entities like internet service provider networks, large corporate networks or key government networks.

(v) Identity Theft attacks including large-scale spoofing, phishing and social engineering attacks which can target users of banks, large e-commerce organizations, key e-governance entities, etc. and lead to loss of sensitive personal data, monetary loss and loss of image and trust.

(vi) Denial of service attacks and distributed denial of service attacks which can cause total or partial disruption of public utility services like fire and water supply.

(vii) Domain name server attacks which can target country level domain registry systems like N1X1 "'.IN" registry

(viii) Application level attacks, i.e., exploitation of inherent vulnerabilities in the code of application software like the web, mails or databases, which can target e-governance, e-commerce, business and banking applications.

(ix) Infrastructure attacks, i.e., Attacks such as denial of service attacks, distributed denial of service attacks, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralised or Distributed Control System (DCS), Gateways of internet service providers and data networks, infection o Programmable Logic Control (PLC) systems by sophisticated malware such as Stuxnet, leading to total or partial disruption of services o; activities in one or more critical sectors such as energy, transport telecommunications and emergency services.

(x) Router Level attacks which can target gateway/ internet service provider routers, routers of large and key economic targets like bank networks and corporate networks and Wi-Fi Routers used by small offices and home users, which can lead to total or partial disruption of internet traffic or online economic activities.

(xi) Cyber Espionage targeting sensitive government organizations, defence and corporate organizations which can lead to disclosure of sensitive information, data theft and compromise of critical internal systems.

Incidents of Cyber terrorism: The increasing reports of cyber terrorism in India and around the world indicate the wide range of facilities which are vulnerable to it because of the use of IT. Reports of cyber terrorism around the world include the July, 2009 cyber-attacks against the US and South Korea, the Estonia 200' cyber-attacks and the Georgia 2008 cyber-attacks where the internet servers, government and political agencies, e-banking services, etc., were attacked through distributed denial of service attacks, mass e-mail, spamming and website defacement. Another form of cyber-attack was the landing of a US unmanned aerial vehicle (UAV) in Iran by a spoofing attack through the feeding of false information to the drone. Apart from these, the onset of viruses like Stuxnet and Duqu which are directed at industrial sabotage are a major concern. Alarmingly, the Stuxnet virus was first used to attack Tehran's nuclear programme, which destroyed its nuclear centrifuges by attacking the PLCs in 2010.

In India, attacks similar to those described above have been carried out. A total of 90 in 2008, 119 in 2009, 252 in 2010 and 219 in 2011 Indian government websites have reported to have been hacked. Currently, the Delhi police has been directed by the courts in an application (titled Tanikella Rastogi Associates v. State) under Sections 156(3) and 200 of the Criminal Procedure Code to investigate the hacking of hundreds of Indian and international websites, including critical government websites, by Pakistan based group of hackers Pak Cyber Eaglez. Another example is the hacking of the systems of the DefenceResearch and Development Organisation (DRDO) in 2013. This led to the leak of thousands of confidential documents relating to Cabinet Committee on Security (CCS), the country's highest decision-making body on security affairs to a server in China.

The use of computers in the carrying out of the 26/11 attacks in Mumbai intensified the need for a legislation dealing with cyber terrorism, and this was part of the reason for the passing of the Amendment Act which introduced the provisions dealing with cyber terrorism. However, these provisions are still inapplicable to the actual use made of the IT by the terrorists, who did not attack the computers or IT systems, but, instead exploited them to aid their purpose. For instance, conventional cell phones and VoIP were used to command and control the attack, Google Earth was used to plan the mission, a picture posted on the Internet of commandos landing on the roof of the hotel was used by the terrorists to ambush the attack and the computer databases of the hotel were accessed to identify and kill guests from other countries like the US and UK. The use of computers in the 26/11 attacks indicates an indirect from of cyber terrorism, where the easily and publicly available information on computers was used for perpetrating terrorism. The provisions of the IT Act in its present form do not deal with this form of cyber terrorism.

Section 66F along with Sections 70, 70A and 70B comprise the sections of theIT Act dealing with cyber terrorism.

Section 66F: Cyber terrorism: Section 66F of the IT Act reads as follows:

"(1) Whoever,-

(A) with intent to, threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a compute resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life. "

Clause 1(A) deals with cyber terrorism that directly affects or threatens to affect the people. The first requirement is an intention to threaten the unity, integrity, etc. of the nation, or to strike terror in the people. With this intention, amrc3ftfle"following acts may be committed:

(i) Denial of access,

(ii) Unauthorised access, and

(iii) Introduction of a computer contaminant.

The result of this denial of access, unauthorised access, or introduced contaminant, may be either to cause or be likely to cause death, injuries to persons, damage or destruction of property, damage or disruption of supplies or services essential to the life of the community, an adverse effect on the critical information infrastructure specified under Section 70 of the Act.

Clause 1(B) deals with cyber terrorism that affects the State. This clause requires intentional or knowing unauthorised access of a restricted, information, data or computer database. The access to such information, data or database must be either restricted for reasons of State security/ foreign relations or the access must be made with the knowledge that it will be used for:

(a) injuring interests of the sovereignty and integrity of India, the security / of the State or friendly relations with foreign States, or
(b) public order, decency or morality, or
(c) in relation to contempt of court, or
(d) defamation, or
(e) incitement to an offence, or
(f) the advantage of any foreign nation/ group of individuals/ otherwise.

The prescribed punishment under this section is imprisonment upto life.

Section 70: Protected system: Section 70 of the IT Act reads as follows:

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (I)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system."

A protected system under this section is a computer resource that:

(i) is declared as such by Notification in the Official Gazette, and

(ii) directly or indirectly affects the facility of a computer resource forming a part of critical information infrastructure, and

(iii) if such a computer resource is incapacitated or destroyed, it will have a debilitating impact on national security, economy, public health or safety.

Any person who gains or attempts to gain unauthorised access to a protected system will be punishable with imprisonment of upto 10 years and also may be jg liable to fine

1. **Critical Information Infrastructure:** Critical information infrastructure (CIIs) is defined in the Explanation to clause (1) as a computer resource, the incapacitation or destruction of which will have debilitating impact on national security, economy, public health or safety. This term has been explained by the National Critical Infrastructure Protection Centre (NCIIPC) as follows:

"The Information Infrastructure is the term usually used to describe the totality of inter-connected computers and networks, and the essential information flowing through them. There are certain parts of the Information

Infrastructure, which are especially critical. The potentiality of such Information Infrastructure makes them important for the economic prosperity of the people and unity and integrity of the Nation. These are the Data Networks which monitor and control important Governmental and Societal functions and services. These include electricity distribution, telecommunication, banking, rail, defence, air traffic etc.

The threats to CIIs range from terrorist attacks to organized crimes to espionage and malicious cyber activities. The various sub-parts of CIIs, such as e-mail services, web services, client services, Wi-Fi services, DMZ services, network services, VOIP services, VPN services, SCADA services, etc., are also continuously susceptible to cyber-attacks.

3. **Declaration of Protected Systems by Notification:** Protected systems are to be declared as such by notification by the 'appropriate Government, in the Official Gazette. Examples of such declarations are:

(i) The Government of TamilNadu declaredin2005thatany computer, computer system, website, online service or computer network including the URL in any of the Offices of the Tamil Nadu Government/ Government undertakings /Boards is protected systems.

(ii) The Central Government declared in 2010 that the TETRA Secured Communication System Network and its hardware and software installed at specified places like the Traffic Control Room (Delhi Police), Jawahar Lai Nehru Stadium (New Delhi), etc. was a protected system.

Declaration as Protected System amounts to Copyright: In the case of B.N. Firos v. State of Kerala, the Government of Kerala had issued a notification declaring ane-government software called 'FRIENDS', which was developed by the petitioner under contract, as a protected system. The petitioner filed a writ petition challenging Section 70 of the IT Act and the notification as being, unconstitutional and inconsistent with the Copyright Act. It was held that a notification under Section 70 of the IT Act is a declaration of copyright under Section 17(d)of the Copyright Act. It was further held that only a compute resource that amounted to a 'government work' under the Copyright Act could be declared to be a 'protected system' under the IT Act:

> *"Section 70 of the Information Technology Act is directly related to Sections 2(k) and 17(d) of the Copyright Act and Government's authority to notify the system as a protected system applies only to such of the system of "Government work".*
>
> *Section 70 of the IT Act is not against but subject to the provisions of the Copyright Act and Government cannot unilaterally declare any system as "protected" other than "Government work" falling under Section 2(k) of the Copyright Act on which Govt. 's copyright is recognised under Section 17(d)of the said Act."*

Section 70 A National Nodal Agency: Section 70A of the IT Act reads as follows:

> *(1)* *The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.*
>
> *(2)* *The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.*
>
> (3) *The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed."*

The National Nodal Agency is the body designated by the Central Government for the purposes of protection of the critical information infrastructure, including research and development. The National Critical Infrastructure Protection Centre (NCIIPC) the National Technical Research Organisation (NTRO) has been designated as the nodal agency under this section[76].The IT National Critical Information Infrastructure Protection Centre and .Manner of Performing Functions and Duties) Rules, 2013, which were issued under sub-clause (3) of this section, prescribe its functions and duties under Rule 4.

Guidelines for Protection of National Critical Information Infrastructure: The NCIIPC has issued "Guidelines for Protection of National Critical Information Infrastructure". These guidelines have prescribed 40 'controls' or guidelines which are to be followed by the CIIs for their protection, such as the Identification of CIIs, Information Security Policy, Data Loss Prevention, Access Control Policies, etc.

Section 70 B: Indian Computer Emergency Response Team to serve as national agency for incident response: Section 70 B of the IT Act reads as follows:

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (I) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

a) collection, analysis and dissemination of information on cyber incidents

b) forecast and alerts of cyber security incidents

c) emergency measures for handling cyber security incidents

d) Coordination of cyber incidents response activities

e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

f) such other functions relating to cyber security as may be prescribed

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (I) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1)."

The Indian Computer Emergency Response Team (CERT-In) was originally established in 2003 and has been operational since 2004. This section empowered the CERT-In to serve as the national nodal agency for the purposes of cyber security. It is responsible for responding to computer security incidents as and when they occur. Its duties have been prescribed under sub-clause (4) of this section:

(i) Collection, analysis and dissemination of information on 'cyber incidents.

(ii) Forecast and alerts of 'cyber security incidents.

(iii) Emergency measures for handling 'cyber security incidents'.

(iv) Coordination of 'cyber incidents' response activities.

(v) Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, and response and reporting of 'cyber incidents.

(vi) Such other functions relating to 'cyber security' as may be prescribed.

The functions of the CERT-In as performed by it have been outlined in the Crisis Management Plan for Cyber Attacks issued by the Ministry of Communications and Information Technology:

(i) The CERT-In scans the Indian cyber space to detect traces of any untoward incident that poses a threat to the cyber space.

(ii) CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, and web defacements, open proxy servers and in carrying out relevant research and development.

(iii) Sectoral CERTs have been functioning in the areas of Defence and Finance for catering critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

(iv) CERT-In has published several Security Guidelines[85] for safeguarding computer systems from hacking and these have been widely circulated All Government Departments/ Ministries, their subordinate offices and. public sector undertakings have been advised to implement these guidelines to secure their computer systems and information technology infrastructure.

(v) CERT-In issues security alerts, advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness.

The IT (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, have been issued under sub-clause (5) of this section. Further, the IT (Salary, Allowances and Terms and Conditions of

Service of the Director General, Indian Computer Emergency Response Team) Rules, 2012 have been issued under sub-clause (3) of this section.

Publishing of Obscene Material

Obscenity: The concept of obscenity can be understood under the following points:

1. Evolution of International Tests for Obscenity: Obscenity is a highly relative concept, with notions of obscenity varying from place to place and person to person. As a result, there is no legal definition for obscenity, nor are there any fixed parameters for judging obscenity. The Courts have laid down some tests which presently serve as guidelines for judging obscenity. The result produced by the application of these guidelines varies from case to case.

(i) Hicklin Test: In the case of Regina v. Hicklin the test for obscenity was laid down as whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall.

This test questioned the effect of certain isolated passages- of the text in question on persons whose 'minds are open to immoral influences'. Though, primarily, reference was being made to the youth, the effect on older persons was also considered, if it was quite certain that the passages would suggest to me minas of the young of either sex, or even to persons of more advanced years, thought of a most impure and libidinous character.'

(ii) Test laid out under United States v. One Book Entitled 'Ulysses': In this case, the criterion for obscenity was 'whether a publication taken as a whole has a libidinous effect'.

This case broadened the Hicklin test, stating that a work to be judged for obscenity was to be considered in its entirety, as opposed to judging the effect of isolated passages.

(iii) Test laid out under Roth v. United States: In this case, the standard for judging obscenity was 'whether, to the average person, applying contemporary community standards, the dominant theme of the material, taken as a whole appeals to prurient interest.

This test requires that the 'dominant theme' of the entire text be of a prurient nature and its effect on the 'average person' of society was to be taken into consideration. This test rejected the Hicklin test on the grounds that the judgment of obscenity based on the effect of a few isolated passages on a susceptible person may result in the rejection of even a legitimate text dealing with such a subject.

(iv) Miller Test: The case of Miller v. California laid down a 'three-prong' test for the evaluation of obscenity:

(a) Whether 'the average person, applying contemporary community standards' would find that the work, 'taken as a whole,' appeals to 'prurient interest'?

(b) Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law?

(c) Whether the work, 'taken as a whole,' lacks serious literary, artistic, political, or scientific value?

Under this test, on fulfillment, of all three criteria, the material in question can be declared to be obscene. For the first two criteria, whether the matter 'appeals to the prurient interest', or is 'patently offensive' is to be determined on the basis of what is acceptable by local contemporary society, or the state, as opposed to a national standard. For the third criterion, whether the work as a whole has any literary, scientific, political or artistic value, as per the notions of a reasonable person (and not an average person of contemporary society) is to be considered.

1. **Indian Judgments on Obscenity:** Some important provisions against obscenity under Indian laws are:

(i) Section 292, IPC: Sale, etc., of obscene books, etc.

(ii) Section 293, IPC: Sale, etc., of obscene objects to young person,

(iii) Section 3, the Indecent Representation of Women (Prohibition) Act, 1986: Prohibition of advertisements containing indecent representation of women.

(iv) Section 4, the Indecent Representation of Women (Prohibition) Act, 1986: Prohibition of publication or sending by post of books, pamphlets, etc., containing indecent representation of women.

Section 292 of the IPC which bans the sale, distribution, renting, exhibition or circulation of obscene material provides a definition of obscenity) in its first clause which bears a huge resemblance to the international tests of obscenity:

> *(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."*

A study of these tests along with the Indian case laws adopting them for the interpretation of Section 292 is necessary for a better understanding of 'obscenity' as used under the related sections of the IT Act:

Ranjit D.Udeshi v. State of Maharashtra

(Adoption of the Hicklin Test)

In this case, Section 292 of the IPC was challenged as being violative of the fundamental right to freedom of speech and expression under Article 19 of the Constitution of India. Here, the Court adopted the Hicklin test to uphold its constitutionality as a law imposing a reasonable restriction on the right to freedom of speech and expression on the grounds of decency and morality, as permissible under clause (2) of Article 19. This clause, in fact, embodies the most fundamental law against obscenity in India.

In its discussion on the Hicklin test, the Court laid down the following guidelines on the basis of which obscenity was to be judged:

(i) Consider both the work as a whole and the effect of the obscene matter by itself, to judge whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort.

(ii) The interests of contemporary society and particularly the influence of the material on this society must not be overlooked.

(iii) Where obscenity and art are mixed, either the art must be so dominant that it overshadows the obscenity or the obscenity must be so trivial and insignificant that it can have no effect and may be overlooked.

(iv) If the obscenity has a dominant social purpose or profit, then it may be overlooked.

(v) A balance must be maintained between "freedom of speech and expression" and "public decency or morality"; but when the latter is substantially transgressed then the former must give way.

Samaresh Bose v. AmalMitra

(Need for objective assessment of obscenity)

In this case, the Supreme Court observed that the concept of obscenity is molded to a very great extent by the social outlook jot the people who are generally expected to read the book. It usually differs country to country depending on the standards of morality of contemporary society in different countries. In consideration of the need to ensure that an objective assessment was made of the obscenity of the material at hand, it discussed the manner in which the assessment could be made independent of each Judge's individual outlook:

(i) The Judge should first place himself in the position of the author and try to understand what the author intends to convey and whether that has any literary or artistic value.

(ii) Then the Judge must place himself in the position of the readers of the book of every age group and try to understand what possible influence the book will have on their minds.

(iii) A Judge should thereafter apply his judicial mind dispassionately to decide whether the book in question can be said to be obscene within the meaning of Section 292 of the IPC.

(iv) For the elimination of any subjective or personal influence on a proper objective assessment, the Judge can, in appropriate cases, refer to the evidence on record and the opinions of reputed or recognized authors of literature.

Some other important points discussed in this judgment which aid the understanding of obscenity are:

(i) 'To deprave' meant to make morally bad, to prevent, to debase or corrupt morally

(ii) 'To corrupt' meant to render morally unsound or rotten, to destroy the moral purity or chastity, to pervert or ruin a good quality, to debase, to defile.

(iii) A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom, but, does not have the effect of depraving, debasing and corrupting the morals of any reader of the novel, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences.

Director General, Directorate General of Doordarshan v. Anand Patwardhan & Anr

(Adoption of the Miller Test)

In this case, the Supreme Court expressed concern at the liberal decision in the case of Samaresh Bose, which essentially gives the judge the power to decide what he or she thinks is obscene. The Court then adopted the three-prong Miller test in place of the Hicklintest for the determination of obscenity.

Ajay Goswami v. Union of India

(Test of Ordinary Man and Contemporary Standards in the Internet Age)

While evaluating the tests for obscenity, the court held that the test for judging a work should be that of an ordinary man of common sense and prudence and not an "out of the ordinary or hypersensitive man".

With reference to the need for consideration of contemporary standards, the Court observed the out datedness of the established tests of obscenity in the internet age:

> *"In judging as to whether a particular work, is obscene, regard must be had to contemporary mores and national standards. While the Supreme Court in India held Lady Chatterley's Lover to be obscene, in England the jury acquitted the publishers finding that the publication did not fall foul of the obscenity test. This was heralded as a turning point in the fight for literary freedom in UK. Perhaps "community mores and standards " played a part in the Indian Supreme Court taking a different view from the English jury. The test has become somewhat outdated in the context of the internet age which has broken down traditional barriers and made publications from across the globe available with the click of a mouse."*

Maqbool Fida Hussain v. Raj Kumar Pandey

(Strict Liability for Obscenity)

This case dealt with the issue of whether, the controversial 'Bharat Mata' minting by M.F. Hussain was obscene under Section 292 and 294 under the IPC. While evaluating the tests for obscenity as laid down in the Ranjit Udeshi case and other important judgments, the Court observed that knowledge was not part of the guilty act, i.e., the offender's knowledge of the obscenity of the matter was not required under the law and it was a case of strict liability in view of this, the obscenity contemplated under these sections of the IPC was not to be equated with the dictionary definition of obscenity which takes within its fold anything which is offensive, indecent, foul, vulgar, repulsive etc. To fall within the scope of 'obscene' under Section 292 & 294 IPC, the ingredients of the matter/art under consideration must lie at the extreme end of the spectrum of the offensive matter.

Section 67: Punishment for Publishing or Transmitting Obscene Material in Electronic Form: The following are some essential elements of this section -

Section 67 prior to Amendment: Prior to the amendment, section 67 read as follows:

> *"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."*

Section 67 prior to amendment was the sole provision of the IT Act dealing with obscene publications. This would include all forms of obscene publications, including those that dealt with pornography - and child pornography. The prescribed punishment was upto 5 years and Rupees 1 lakh. For the first conviction and upto 10 years and Rupees '2 lakhs for a subsequent conviction. With a view of bringing the IT Act in tune with legislations prevalent in other advanced democracies, this section was amended to introduce more stringent provisions for pornography, and especially for child pornography.

[Section 67 of the IT Act in its current form deals with publishing of 3scene information, Section 67A of the Act deals with publishing of sexually explicit/ pornographic material and Section 67B of the Act deals with child pornography.

Section 67 reads as follows:

"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter –contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees."

This section has been framed along the same lines as Section 292 of the IPO This will apply when the obscene material is published or transmitted in an electronic form. The prescribed punishment for a first conviction was changed to imprisonment upto 3 years, fine upto Rupees 5 lakhs or both. The punishment for a second conviction was changed to imprisonment of 5 years, fine of Rupees 11 lakhs or both.

'Obscenity': For the term 'obscenity' under this section, reference should be made to the judgments discussed above for the interpretation of obscenity under Section 292 of the IPC. The Supreme Court in the case of Maqbool Fidi Hussainv. Raj Kumar Pandey[1], observed that the tests for obscenity under this in section and Section 292 of the IPC were similar:

"...Section 67 is the first statutory provisions dealing with obscenity on the Internet. It must be noted that the both under the Indian Penal Code, 1860 and the Information Technology Act, 2000 the test to determine obscenity is similar."

An exception has been made for obscene information that is published for the public good or which is used for religious/ heritage purposes.

Publish, Transmit or Cause to be published': This section criminalizes only the publication and transmission of obscene material. The downloading, viewing possessing etc. of obscene material is not an offence under this section (unlike under Section 67B). Publication' of a material refers to its dissemination or circulation. In the absence of any other definitions under the IT Act, reference may be made to the explanations of 'publish' and 'transmit' under Section 66E of the IT Act, where/publication refers to the electronic or physical reproduction of the material and the making of these reproductions accessible to the public. This section criminalizes both the direct and indirect publication of obscene material. Transmission under Section 66E of the IT Act refers to an intentional electronic transfer of the material so that it can be viewed by another person or persons. The meaning of these terms was discussed under the case of Avinash Bajaj v. State (NCT) of Delhi (the Baazee case), wherein obscene material was put up for sale by one person on the website Baazee.com and sold to several other people. The issue for the purposes of Section 67(prior to amendment)of the Act was whether (he website had indirectly published the material, i.e., did it 'cause the publication' of the material. For this purpose the Court drew up the following chain of transactions' for the publication and ultimate transmission of the material on sale through the website:

(i) Once the interested buyer gets on to Baazee.com and views the listing, he then opts to buy the said product and then makes payment.

(ii) Only then the remaining part of the chain is complete and the product, which in this case is the video clip in electronic form, is then transmitted through an email attachment and then can get further transmitted from one person to another.

(iii) The video clip sent as an email attachment can straightway be downloaded onto to the buyer's hard disc and numerous copies thereof can be made for further transmission.

(iv) The 'publishing' in this form is therefore instantaneous and can be repeated manifold.

In fact in the present case, the transmission of the clip to eight buyers located in different parts of the country took place in a very short span of time.

In view of this 'chain of transactions', the Court held that, the ultimate transmission of the obscene material wouldn't have been possible without the initial facilitation by the website, and therefore the website had prima facie 'caused' the publication:

> "...it cannot be said that baazee.com in this case did not even prima facie "cause" the publication of the obscene material. The ultimate transmission of the video clip might be through the seller to the buyer but in a fully automated system that limb of the transaction cannot take place unless all the previous steps of registration with the website and making payment take place. It is a continuous chain."

Presumption of Knowledge under Section 67: Section 67 of the IT Act is silent of on the requirement of mensrea, i.e., there is no requirement of the publication, transmission or indirect publication to have been done intentionally or knowingly, etc. The general rules of interpretation for a provision of criminal law are silent on mensrea, are outlined below:

(i) If a section is silent as to mensrea, there is a presumption that words importing mensrea must be read into the section in order to give effect to the will of the Parliament.

(ii) If a penal provision is capable of two interpretations, the one which is most favourable to the accused is to be adopted.

(iii) The fact that other sections of the Act expressly require mens red does not in itself imply that a section silent with respect to mensrea creates an absolute offence.

Therefore, as per these rules, though the lack of mensrea in Section 67 of the IT Act indicates that it imposes strict liability on a publisher or transmitter, such an assumption cannot be made exclusively on this basis. This assumption can, however be made based on the strict liability imposed under Section 292 of the IPC, which is also similarly silent on mensrea. In Ranjit D. Udeshiv. State of Maharashtra, discussed above, the Court held that, for an offence under Section 292 of the IPC, the prosecution was not required to prove that the accused had knowledge that the material on sale, etc. was obscene. In the Baazeecase, the Court observed that 'in view of the strict liability imposed under Section 292', the website's knowledge of the obscene material was presumed. The Court further held that this presumption, however, was rebuttable, and it was a matter of evidence to prove that the website had exercised due care to prevent the publication or transmission.

In view of this general rule of interpretation and the interpretation of Section 292 of the IPC in the Baazeecase, it can be assumed that a similar rebuttable presumption of knowledge exists in case of a person accused under Section 67 of the IT Act.

Any material': The term 'any material' implies that the section covers obscene material in any 'electronic form', i.e., images like photographs, morphed images, audio files, video files, of software programmes and text messages like e-mails, SMSs and through instant messaging.

State of Tamil Nadu v. Suhas Kaitf

(First conviction under Section 67)

This case is considered to be the first ever conviction under Section 67 of the IT Act in India. Some obscene, defamatory and annoying messages were posted on a Yahoo messaging group about the victim, who was a recently divorced woman.

This message resulted in annoying phone calls to the victim. Upon filing an FIR the accused, who was a former family friend of the victim was arrested and found guilty for offences under Sections 469 and 509 of the IPC, and Section 67 of the IT Act.

Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc. in electronic form: Section 67A of the IT Act reads as follows:

"Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or oviduct shall be punished on first conviction with imprisonment of either description for a term which mm extend to five years and with fine which may extend to ten lakh rupees and an the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Similar to Section 67, Section 67 A of the IT Act criminalizes the publication $_a$nd transmission of sexually explicit material in an electronic form, but it's viewing, downloading, possession, etc. is not an offence. The punishment prescribed is higher than that under Section 67 of the Act.

The term "sexually explicit" generally refers to pornographic content. It has been qualified by the term 'explicit', indicating that it refers to something which is more than just obscene[10]. Also, Section 67A of the Act does not apply the 'l^^p1vJmdience' test used in Section 67 of the Act, i.e., it does not take the effect of the material on the people who are likely to read, see or hear the material into consideration. This implies that the section refers to matter that is patently or grossly explicit. The exception for information that is published for the public good, or which is used for religious or heritage purposes is applicable to Section67Aofthe Act as well.

Though, the IT Act does not criminalize the viewing, downloading, browsing, etc. of this material, steps have been taken by the Government to prevent this. The most recent step is the internet censorship through a Department of Telecom order dated 13th July 2013, whereby 39 websites which host or allow their users Ho share obscene content were blocked. This order was issued to comply with a direction from the Supreme Court in response to a petition seeking an anti-pornography law[13]. This restriction on pornographic content is also evident under certain rules issued by the Government:

(i) **No hosting, displaying, etc. of pornographic information:** Rule 3 (2) (b) of IT (Intermediary Guidelines) Rules, 2011, requires the intermediary to inform users not to host, display, upload, modify, publish, transmit, update or share any information that is obscene, pornographic or pedophilic.

(ii) **Software to filter out pornographic websites:** Rule 6 (5) of the IT (Guidelines for Cyber Cafe) Rules, 2011, requires cyber cafes to be equipped with safety of filtering software to avoid access of websites relating to pornography, cyber pornography or obscene information.

(iii) **Prohibit viewing of pornography:** Rule 6(5) of the IT (Guidelines for Cyber Cafe) Rules, 2011, requires cyber cafes to display a board to users prohibiting them from viewing pornographic sites.

State of Tamil Nadu v. Dr. L. Prakash

This was a landmark case where the accused, a renowned doctor in Tamil Nadu was convicted for the creation of pornographic videos using his patients and posting the pictures and videos on the internet. The accused was charged under various sections of the IPC, Immoral Traffic (Prevention) Act, 1956 and the Indecent Representation of Women (Prohibition) Act, 1986. In view of the gravity of the offence, a life sentence was awarded to the doctor under the Immoral Traffic (Prevention) Act, 1956.

Section 67 B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: The following are the important elements for this section:

1. International Measures for Protection of Children: The provisions in some important international instruments dealing with the sexual exploitation of children, including their abuse, trafficking and child pornography are:

(i) UN Convention on Rights of Child: India ratified this convention on 11 December 1992. The term 'all forms' of sexual exploitation indicates that this Convention also applies to online sexual exploitation.

(a) Article 34 of the Convention directs the protection of children from 'all forms' of sexual exploitation and abuse.

(b) Article 34 of the Convention also directs the taking of national, bilateral and multilateral measures to prevent the use of a child in any unlawful sexual activity for prostitution or pornography.

(c) Article 35 of the Convention mandates the taking of measures to prevent the sale or trafficking of children.

(d) Article 36 of the Convention mandates the protection of children from 'all other forms of exploitation'.

(ii) Budapest Convention on Cyber-crime: India is not a signatory to this Convention. However, Section 67B of the IT Act was drafted taking special note of Article 9 of the said Convention which deals with child pornography. The following are its important provisions:

(a) Article 9 of the Convention mandates the adoption of legislative and other measures to criminalize the production, offer, distribution, transmission, procurement or possession of child pornography through a computer system

(b) Article 9 of the Convention defines 'Child Pornography' to include a visual depiction of a minor, a person appearing to be minor or realistic representations of a minor engaged in sexually explicit conduct.

(iii) SAARC Convention on Preventing and Combating the Trafficking in Women and Children for Prostitution: Indian ratified this Convention on5th January, 2002. This Convention will be relevant in cases where the children are trafficked within India or within South Asian countries, and are used' for the purposes of online sexual exploitation. This Convention also includes detailed provisions for extradition and mutual legal assistance between parties, like the following:

(a) Article I, Point 3 of the Convention defines "Trafficking" as the moving, selling or buying of women and children for prostitution within and outside a country for monetary or other considerations with or without the consent of the person subjected to trafficking.

(b) Article I, Point 5 of the Convention defines "Persons subjected to trafficking" as women and children who are victimised or forced into prostitution by any unlawful means, such as deception, threat, coercion, kidnapping, sale, fraudulent marriage, child marriage, etc.

(c) Article IV of the Convention mentions the victimization or trafficking of children as an aggravating circumstance for an offence under this Convention.

(iv) Optional Protocol to UN Convention on Rights of Child on Sale of Children, Child Prostitution and Child Pornography: India ratified this Protocol on 16th August, 2005. Even in the absence of a specific mention of use of a computer, the definition of child pornography, which includes representation by 'whatever means', will include a representation in an electronic form. More importantly, this Convention includes provisions with respect to extradition and assistance in investigation and other criminal proceedings between signatories to the Protocol.

(a) Article 2(b) of the Convention defines "child prostitution" as the use of a child in sexual activities for remuneration or any other form of consideration.

(b) Article 2(c) of the Convention defines "child pornography" as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

(c) Article 3 of the Convention criminalizes the producing, distributing, disseminating, importing, exporting, offering, selling or possessing of child pornography.

(v) Palermo Protocol - UN Protocol to Prevent, Suppress and Punish Trafficking in - Persons, Especially .Women and Children, supplementing the United Nations Convention against Transnational Organized Crime: India ratified this Protocol on 5 May, 2011.This protocol provides a very comprehensive definition of the term 'trafficking' and the means by which it is achieved.

(a) Article 3(a) of the Convention defines "Trafficking in persons" to mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of force/ coercion/abduction/ fraud/ deception/ the abuse of power/ the abuse of a position of vulnerability/ the giving or receiving of payments to achieve the consent of a person having control over another person, for the purpose of exploitation.

(b) Under Article 3(a) of the Convention, "exploitation" includes the exploitation of the prostitution of others or other forms of sexual exploitation.

(c) Under Article 3(b) of the Convention, the consent of the trafficked victim is irrelevant if brought about by these means.

2. ***Indian Laws Against Sexual Exploitation of Children:*** Many Indian laws contain provisions protecting children against sexual abuse, prostitution, trafficking, pornography, etc. Some of the important provisions are:

(i) The Constitution of India: The most fundamental protections to children against sexual exploitation are embodied in the Constitution:

(a) Article 21 protects life and personal liberty.

(b) Article 23(1) prohibits traffic in human beings.

(c) Article 39(f) directs the state to ensure that children are protected against exploitation.

(ii) The Indian Penal Code, I860: Sexual offences in general, applicable to both minors and adults are covered under the IPC. The IPC also contains certain provisions specific to minors for their use in prostitution or illicit intercourse:

(a) Section 372 punishes the selling, letting, etc. of a minor for prostitution, illicit intercourse, or any unlawful or immoral purpose with imprisonment upto ten years and fine.

(b) Section 373 punishes the buying, hiring, etc. of a minor for prostitution, illicit intercourse, or any unlawful or immoral purpose with imprisonment upto ten years and fine.

(c) Section 366A punishes the procurement of a minor girl for illicit intercourse with imprisonment upto ten years and fine.

(d) Section 366B punishes the importation of a girl under 21 years of age from a foreign country for illicit intercourse with imprisonment upto ten years and fine.

(iii) The Immoral Traffic (Prevention) Act, 1956: This Act deals with immoral traffic for the purposes of sexual exploitation in brothels and other similar premises. The Act also contains detailed provisions for the use of a child for prostitution:

(a) Section 2(f) of the Act defines 'prostitution' as the sexual exploitation or abuse of persons for commercial purposes or for consideration in money or in any other kind.

(b) Section 4 of the Act punishes a person living on earnings of the prostitution of a child with imprisonment of 7 to 10 years.

(c) Section 5 of the Act punishes the procurement, inducement or taking of a child for the sake of prostitution with rigorous imprisonment of a minimum of 7 years upto life.

(d) Section 6(2) of the Act relates to the detention of a child in a brothel.

(e) Section 7(1) of the Act punishes prostitution carried on with a child in the vicinity of a public place with 7 years upto life, or 10 years with fine.

(f) Section 7(2) of the Act deals with the case of prostitution being permitted with respect to a child in a hotel.

(iv) The Protection of Children from Sexual Offences Act, 2012: ThisActwasenactedrecentlytoimplementArticle34oftheConvention on the Rights of Child, which required the introduction of national measures to prevent the sexual exploitation of children. It is the first law in India which deals specifically with offences against children. The need for this specific legislation arose because the IPC sections on sexual offences do not cover all types of offences against children, and more importantly do not distinguish between children and adults. The Act prescribes offences with respect to sexual harassment, sexual assault and pornography involving children with varying punishments depending on the gravity of the crime It is important to note that Section 13 of the Act also includes online exploitation of children. Some of the key provisions are:

(a) Section 3 of the Act defines a 'penetrative sexual assault' and Section 7 of the Act defines 'sexual assault'.

(b) Section 5 of the Act punishes aggravated penetrative sexual assault, such as assault by police officer, staff of educational or religious institution or a relative with rigorous imprisonment of a minimum of ten years and upto life, along with a fine.

(c) Section 9 of the Act punishes aggravated sexual assault with simple or rigorous imprisonment of a minimum of 5 years upto 7 years and fine.

(d) Section 11 of the Act defines 'sexual harassment' which includes enticing the child using or for pornography and stalking the child.

(e) Section 13 of the Act defines the use of a child for pornographic purposes as use of the purposes of sexual gratification in any form of media, including the internet, electronic form, *etc.*

(f),The explanation to Section 13 of the Act explains that the term 'use a child' shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of pornographic material.

(g) Section 21 of the Act mandates the reporting of an offence under the Act and failure to do so is punishable with 6 months imprisonment and/ or fine.

(h) Chapter VII establishes Special Courts for trial of offences under the Act.

v) Advisory on Preventing & Combating Cyber Crime against Children: This advisory was issued by the Ministry of Home Affairs in 2012 to the states for steps to be taken for matters such as the protection of children from cyber-crime , dealing with children committing cyber-crime and conduction of investigations.

(a) Special Juvenile Police Units constituted under Section 63 of Juvenile Justice (Care and Protection of Children) Act, 2009 to be sensitized and trained to deal with children in conflict of law with respect to cyber-crimes as well.

(b) Implementation of 'parental control software' to mitigate spoofing of age, gender and identity to prevent access to obscene material.

(c) Training to law enforcement agencies such as the police, judiciary and examiners of digital evidence.

(d) Police to carry out undercover cyber patrol operations to identify cyber criminals in accordance with Sections 72 and 72(A) of IT Act

(e) For investigations requiring help from outside India, approach CBI Interpol Division or contact G8 24x7 Help Desk of CBI. Provisions of Mutual Legal Assistance Treaties and Letter of Rogatories (LR) may be used.

Prior to the IT Act, the provisions of the IPC and the Indecent Representation of Women (Prohibition) Act were used to deal with issues of pornography. These provisions included visual representations in their scope, but, other electronic materials like audio materials and computer-generated photographs were, not specifically covered. Further, these Acts did not deal with the issue of child sexual abuse and more importantly with child pornography adequately. While the issue of whether pornography and prostitution should be legalized is regularly debated, a line has always been drawn with child pornography and sexual abuse. The IT Act (prior to amendment) introduced some protection for the publication and transmission of obscene materials, but stringent punishment for child pornography and sexual abuse came were still required.

With a view to imposing this stringent punishment and bringing India in line with the international instruments listed above, Section 67 was amended to introduce safeguards against the online sexual exploitation of children through Section 67B. This resulted in the criminalizing of acts like the possession, viewing and creation of child pornography in addition to its publication and transmission. Another important addition is the clause to deal with grooming of children for these purposes.

Section67B-Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: Section 67B of the IT Act reads as follows:

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit actor conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, Shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with

> imprisonment of either description for a term which may extend to seven years and also with fine which may extend to tėn lakh rupees:

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years."

Clause (a) says,

"publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct:"

This clause relates specifically to child pornography, and is similar in its drafting to Sections 67 and 67A of the Act. It punishes the publication, transmission and causing the transmission of an electronic material depicting children engaged in a sexually explicit act or conduct. The terms 'publication', 'transmission' and 'sexually explicit' have been explained in the previous sections. Though this section does not specifically criminalize the publication or transmission of material depicting children which is obscene and not sexually explicit, such material would still be covered under Section 67A of

Material depicting' children

The scope of this clause is not restricted to material involving actual children only. On comparison between this clause and Section 67A of the Act, it can be observed that Section 67B of the Act criminalizes material 'depicting' children in sexually explicit acts, as opposed to Section 67A of the Act, which criminalizes material 'Containing' sexually explicit acts. The use of the word 'depict' indicates the adoption of the explanation of 'child pornography' under Article 9 of the Budapest Convention on Cyber-crime, which states that:

"The term "child pornography" shall include pornographic material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct.

(c) realistic images representing a minor engaged in sexually explicit conduct.

For a better understanding of the scope of 'child pornography' under this Article, reference may be made to the Explanatory Report to the Convention on Cyber-crime:

(i) Types of pornographic material: The three types of pornographic material covered are depictions of sexual abuse of a real child, pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct and images which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct, such as morphed or computer generated images [3].

(ii) Legal interests protected under this clause: The legal interests protected under each clause is different: Clause (a) focuses on direct protection against child abuse, while Clauses (b) and (c) focus on behavior that may indirectly harm the child, such as material which may be used to encourage or seduce the child.

(iii) National standards of pornography: The term 'pornographic material' is to be governed by national standards of what is obscene, immoral, etc.

iv) Data capable of conversion: Visual depiction includes data stored or computer diskette or on other electronic means of storage, which are capable of conversion into a visual image.

(v) Real/ simulated: It is irrelevant whether the 'sexually explicit conduct' is real or simulated.

On the basis of this explanation, it can be assumed that the term material depicting children in sexually explicit act' under Section 67B (c) of the IT Act includes the following-

(a) An actual minor engaged in sexually explicit act or conduct.

(b) A person who appears to be a minor engaged in sexually explicit act or conduct, whether or not such person actually is a minor.

(c) A realistic image representing a minor engaged in sexually explicit act or conduct, such as morphed images, pseudo photographs, simulated or virtual reorientations like animations, cartoons, drawing or paintings.

Clause (b) says,

"creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic .form depicting children in obscene or indecent or sexually explicit manner."

This clause incorporates a total ban on any material that sexually exploits children. It relates to electronic material depicting children in an obscene, indecent or sexually explicit manner. The following acts in relation to such material have been criminalized:

(i) **Creation:** The creation of text or digital images is covered under this clause. This will include the creation of morphed images, pornographic images and written material containing references to children in an obscene, indecent or sexually explicit manner.

(ii) Consumption: The consumption of such material, i.e., the col lection, seeking, browsing and downloading of such material is also included in this section. Therefore, acts like searching for or browsing through child pornography on the internet, downloading, storing it on a computer or in any other electronic form, will be an offence. The reason for banning the consumption of obscene or pornographic material depicting children, while permitting the consumption of other obscene or pornographic material, is due to the fear that allowing it will encourage the actual commission of sexual abuse against children.

(iii) Distribution: The clause also includes any step leading to the spread of such material, such as its advertisement, promotion, exchange or distribution. Some convictions in the U.S. for distribution of such material includes cases of sending e-mails advertising the creation of a Yahoo! Group for sharing child pornography, for publishing a

> notice over the Internet offering to exchange child pornography and for responding by email to an advertisement placed by U.S. Postal Service Inspectors in Internet newsgroups known to be frequented by individuals interested in child pornography.

Clause (c) says,

> "cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource."

This section covers the online solicitation of a child or the grooming of a child for sexual purposes. It must have been the intention of the legislature to include pre-offence grooming by anyone, an adult or a child, which results in an online relationship with this adult or anyone else for the purposes of a sexually explicit act. However, the drafting of the section seems to indicate that its scope is restricted to instances of where the online relationship which the child is being cultivated, enticed or induced into is with another child only and not with an adult. It is not specified whether the person actually doing the grooming is an adult or another child, so long as the purpose is for an online relationship with another child. A clear interpretation of this section is required in order to include grooming in its entirety, and not restrict it to a relationship between children.

Clause (d) says,

> *"facilitates abusing children online"*

This clause covers any act that facilitates or aids the abusing of children online) For example, a person involved in on-line practices like the exchange of ideas, fantasies and advice among pedophiles, or a website that permits such activities, which can play a role in encouraging sexual offences against children, would be covered under this. This clause may also be used against intermediaries such as cyber cafes that omit to take due care.

Clause (e) says,

"records in any electronic form own abuse or that of others pertaining to sexually explicit act with children."

This clause refers to the recording of a sexually explicit act with a child, whether the abuser is the person recording or any other person. This will include any recording in electronic form, such as videotaping, taking photographs through a digital camera or smartphone or recording or photographing through a webcam. The purpose for which the recording is done is irrelevant, i.e., the mere act of recording a sexually explicit act with a child is an offence.

Wilhelmus Weijdeveld .India

This was the first case charged under Section 67B of the Act. Wilhelmus was a Dutch national who came to India as a tourist in 1980 and was running an orphanage. He was arrested in 2002 on receiving a tip-off from INTERPOL thai he was uploading pornographic content. It was found that he was sexually abusing 5 boys in his orphanage.

Avinash Bajaj v. State (NCT) of Delhi

(The Bazeecase)

In this case, the website Bazee.com carried a listing which offered for sale a video clip shot using a mobile phone of two school children indulging in a sexually explicit act. The listing escaped the filters installed in the website, but was brought to the notice of the website on the same day that it was put up by another user. Despite this, the listing was available for sale for a period of 3 days and was thereafter purchased by 8 persons. The key findings of the High Court of Delhi in petition to quash the criminal proceedings against the petitioner were as follows:

(i) Prima facie obscene: The listing contained explicit words that left a person in no doubt that what was sought to be sold was lascivious, and therefore the listing was prima facie an obscene material or text.

(ii) Failure of filters: Website owners and operators need to employ filters if they want to prove that they did not knowingly permit the use of their website for sale of pornographic material. However, if the filters fail, then, the website's knowledge of the obscene material will be presumed under Section 292(1) of the IPC.

(iii) Presumption of knowledge is rebuttable: This presumption of knowledge, however, is rebuttable, and it is a matter of evidence to prove that the website had exercised due care to prevent the publication or transmission.

(iv) Website 'caused' the publication: In view of the chain of transactions, most of which are under the direct control of the website, the website did prima facie 'cause the publication' under Section 67 (prior to Amendment) of the IT Act.

(v) Petitioner not liable in individual capacity. The IPC does not recognise the concept of 'automatic criminal liability' attaching it to the director, where the company is an accused. In the absence of a specific allegation in the charge sheet that despite knowing the failure of the filters, he nevertheless, did nothing about it, the petitioner cannot be held liable in his individual capacity.

(vi) Petitioner is liable in his capacity as MD: Section 85 of the IT Act attaches a deemed criminal liability on a person who, at the time of commission of the offence, was in "charge of, and was responsible to, the company". On this basis, the petitioner is liable in his capacity as the Managing Director.

Proviso to Sections 67, 67A and 67B: The Proviso to Sections 67, 67A and 67Bof the IT Act reads as follows:

"Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

i. The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

ii. which is kept or used for bonafide heritage or religious purposes. "

This excludes the application of Section 67, 67A and 67B of the Act to any and electronic material:

i. Which is in the interest of science, literature, art, learning or any other objects of general concern, and its publication is justified on this account, or

ii. Which is kept or used for bonafide heritage or religious uses.

This section is similar to the first exception provided under Section 292 of the IPC. The first exception has been inserted for the protection of material which is published for the public good, such as material dealing with medical information, art, social causes, etc. For example, the film 'Bandit Queen' was held to be a film that carried a message of social evil, and the depictions of nudity and rape were not obscene or pornographic[42]. The second exception protects material used for religious or heritage purposes, such as the sculptures in the temples of Bhubaneshwar, Konark and Puri in Orissa and Khajuraho in Madhya Pradesh.

Offences Relating to Electronic Signatures: Sections' 68, 7l, 73 and 72 of the IT Act deal with offences relating to Electronic Signatures.

Section 68 - Violation of Controllers' Directions: Section 68 of the IT Act reads as follows:

"(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding .two. years or to a fine not exceeding one lakh rupees or to both."

Under this section ah offence will be committed when certain orders of the Controller are not followed. The orders may be with respect to any issue requiring compliance with the IT Act or Rules, for example, licensing of Certifying Authorities ("CA"), issue of electronic signature certificates or prescribing the standards to be maintained by the CAs. The element of mensrea, i.e., 'intentionally/knowingly' in the second clause, was inserted by the Amendment Act.

Section 71 - Penalty for Misrepresentation: Section 71 of the IT Act reads asfollows:

> "Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may, extend to two years, .or with fine which may be extended one lakh rupees, or with both".

This section criminalizes the obtaining of a license by a CA or an Electronic Signature Certificate by a subscriber by means of:

i) A misrepresentation to the Controller or CA, i.e., any false or inaccurate statement. The section does not specify whether the misrepresentation should have been made with or without an intention to deceive. Therefore, it may include misrepresentations whether made intentionally, negligently or innocently.

(ii) A suppression of a material fact from the Controller or CA, i.e. the concealment of a material fact. A material fact is any information that is sufficiently significant so as to influence an individual into doing something, in this case into issuing the license or Electronic Signature Certificate.

The punishment under this section is in addition to the powers of the Controller to suspend or revoke the license[45] or electronic signature[46] in case of a statement made in the application which is false or a material fact which is concealed.

Section 73 - Penalty for publishing Electronic Signature Certificate false in certain particulars: Section 73 of the IT Act reads as follows:

"(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

This section deals with the publishing or making available of an electronic signature certificate knowing that such" certificate:

(i) is not issued by the CA listed as the issuing authority in the certificate.

(ii) has not been accepted by the subscriber listed in the certificate.

(iii) has been revoked or suspended, unless the publication is for the purpose of verification prior to such revocation or suspension.

Publication of an electronic signature certificate refers to publication in a repository, or publication to another person (for example, by usage of the digital signature) or in any other manner.

Section 74 - Publication for fraudulent purpose: Section 74 of the IT Act reads as follows:

> "Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

This section punishes the creation, publication or making available of an electronic signature for a purpose which is fraudulent, i.e., with the intention to defraud, or unlawful, i.e., which is violative of the law. The phrase 'fraudulent or unlawful purpose' is wide enough to include any contravention under a law for the time being in force[50].

Section 72 - Breach of confidentiality and privacy: Section 72 of the IT Act reads as follows:

"Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

This section confers the right of privacy over any information acquired in official capacity. The disclosure made should be without consent and should not be permitted or required under any other law.

Powers conferred under the IT Act, Rules and Regulations

It is important to note that this section is applicable only to the violation of privacy by a person who obtained the information in exercise of a power conferred under the IT Act, or the Rules and Regulations made there under. Therefore, it applies to authorities such as the Controller, CAs, and their employees and authorised officers of the Central Government. There are several sections which confer such power under the IT Act, for example:

(i) Section 67 C: Intermediary retaining or preserving information.

(ii) Section 68 (1): Directions given by a Controller or Certifying Authority.

(iii) Section 69: Any agency or intermediary directed to intercept, monitor or decrypt any information.

(iv) Section 69B: Any agency or intermediary of the Government authorised to monitor, collect data or information.

(v) Section 79A: The Examiner of electronic evidence.

Right to Privacy not Absolute: The right to privacy is implicit in the right to life and liberty guaranteed under Article 21 of the Constitution. Anything concerning the private matters of a person, whether truthful or otherwise, which is published without his consent amounts to a violation of privacy'. This right to privacy is, however, not absolute. It is subject to restrictions on the grounds of public morality, compelling public interest, and the like[52]. Similarly, the right against breach of confidentiality and privacy conferred under this section and section 72A of the IT Act is subject to any contrary provision of the IT Act or any other act for the time being in force requiring or permitting disclosure.

For example, in the case of Radiological and B Imaging Association v. Union of India, it was sought to prove that a 'silent observer', an electronic device which was attached to a sonography machine for recording and viewing sonography scans was a violation of a patient's right to privacy and confidentiality under Section 72 and 72A of the IT Act. The Court, while emphasizing that the right to privacy was not absolute, held that these sections were not applicable to this case on these grounds:

(i) The provisions of the Pre-conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 and the Rules there under will prevail over the provisions of Sections 72 and 72A of the Act, which are both subject to the provisions of any other law for the time being in force.

(ii) Section 72 of the IT Act applies only to information acquired in exercise of powers conferred under the IT Act, Rules and Regulations made there under.

Section 72A - Punishment for Disclosure of Information in Breach of Lawful Contract: Section 72A of the IT Act reads as follows:

> "Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

This section applies to any person, including an intermediary, who discloses personal information secured through the provision of services under a lawful contract. Section 72 of the IT Act criminalizes the mere disclosure of personal information without consent. However, this section requires the additional element of mensrea, i.e., the intention to cause or knowledge of likelihood of causing wrongful loss or gain.

Section 85 - Offences by Companies: Section 85 of the IT Act reads as follows:

> "(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
>
> Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
>
> (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation-

For the purposes of this section

i. Company means any Body Corporate and includes a Firm or other Association of individuals; and

ii. "Director", in relation to a firm, means a partner in the firm."

This section incorporates the concept of corporate criminal liability, or the criminal liability imposed on a company for its contravention of the IT Act or any rule, direction or order made there under. The explanation to the section provides that a company is anybody corporate, including a firm or association of individuals. The company may be incorporated or unincorporated.

Clause (1) - Liability of person in charge of or responsible to the company: This clause imposes liability on every person who:

(i) at the time of commission of the offence by the company,

(ii) was in charge of, and responsible to the company,

(iii) for the conduct of the business of the company and for the company.

(iv) This liability is subject to the person being proceeded against proving that:

(v) the contravention took place without his knowledge, or

(vi) that he exercised all due diligence to prevent such contravention.

Clause (2) - Liability of person with whose consent, connivance or neglect the offence takes place: This clause imposes liability on:

(i) the Director, Manager, Secretary or other officer,

(ii) and if it is proved that the contravention took place with such person's consent or connivance, or because of its neglect.

This liability is in addition to the liability imposed under clause (1). The explanation to this section provides that for a firm, the director would mean the partner of the firm.

Prosecution of a Company is a Sine Qua Non for Prosecution of Other Persons: Section 85 of the IT Act and sections of other Acts which are in pari material mention the following persons who can be held liable for an offence by a company:

(i) The company,

(ii) Every person who, at the time the contravention was committed, was in charge of, and was responsible to, the Company for the conduct of the business of the Company, and

(iii) Any director, manager, secretary or other officer of the Company with whose consent or connivance or because of neglect attributable to whom the offence has been committed.

Formerly, any one, or more than one or all of the persons could be held liable for the offence. In the case of Sheoratan Agarwal v. State of Madhya Pradesh, it was held that:

"there is no statutory compulsion that the person –in-charge or an officer of the company may not be prosecuted unless he be ranged alongside the company itself. Each or any of them may be separately prosecuted or along with the company if there is a contravention.... By the company.

This position was overruled in a combined decision given by the Supreme Court in the cases of Aneeta Hadav. M/s Godfather Travels and Tours Pvt. Ltd.[56] and the Baazeecase, which laid down that the prosecution of the company was a condition precedent for the prosecution of persons mentioned in the second and third categories, i.e., every person who was in charge of or responsible to the company, and the director or managing director. However, a distinction is to be made between cases where a company had not been made an accused and the one where despite making it as an accused, cannot be proceeded against because of a legal bar. In the latter case, the persons under the second and third categories may be proceeded against if other ingredients of the offence are fulfilled.

In the Baazeecase, the petitioner, who was the managing director of Baazee.com India Pvt Ltd. (BIPL) was prosecuted under Section 292 of the IPC and Section 67 of the IT Act without impleading the company as an accused. The prosecution was challenged under Section 482 of the Criminal Procedure Code, 1973 before the Delhi High Court[57]. The Court noted that the petitioner's responsibilities in the company was that he was in charge for the Indian operations of the Company and was responsible for policy decisions, planning, control and overall supervision of day to day functioning of the organization. This was contrasted with the role of the Senior Manager, Trust and Safety, who were responsible for maintaining the subject and banned key word list and ensuring that no lascivious item is listed for sale on the website. The Court observed that though & prima facie case had been made out against the company, there was no specific allegation against the petitioner in his individual capacity. The court, therefore, held that the liability could be attached to the petitioner only in his capacity as MD under Section 85 of the IT Act and not in his individual capacity under Section 292 of the IPC:

(i) A director does not automatically become criminally liable for the criminal acts of the company.

(ii) In the absence of the company being made an accused and in the absence of specific allegations concerning the MD of the company, it is not possible to make out even a prima facie case against the petitioner in his individual capacity under Section 292 of the IPC.

(iii) A prima facie offence against the company has been made out under Section 67 of the IT Act.

(iv) Without the company being made an accused, its directors can be proceeded against under Section 67 read with Section 85 of the IT Act.

(v) A *prima facie* offence is made out against the petitioner under Section 85. Since, the law recognises the deemed criminal liability of the directors even where the company is not arraigned as an accused and particularly since it is possible that BIPL may be hereafter summoned to face trial.

This decision with respect to Section 85 of the IT Act was overruled in appeal before the Supreme Court[58]. The Court observed that companies can no longer claim immunity from prosecution on the grounds that they were incapable of possessing the required *mensrea* .However, the normal rule in cases involving criminal liability is against the imposition of vicarious liability, subject to an exception on account of a specific provision being made in a statute, which extends liability to others. In such situations the conditions laid down are to be strictly complied with. With respect to Section 141 of the Negotiable Instruments Act, 1881, the Court held that:

> *"...commission of offence by the company is an express condition precedent to attract the vicarious liability of others. Thus, the words "as well as the company" appearing in the Section make it absolutely unmistakably clear that when the company can be prosecuted, then only the persons mentioned in the other categories could be vicariously liable for the offence subject to the averments in the petition and proof thereof...*
>
> *... we arrive at the irresistible conclusion that for maintaining the prosecution under Section 141 of the Act, arraigning of a company as an accused is imperative. The other categories of offenders can only be brought in the dragnet on the touchstone of vicarious liability as the same has been stipulated in the provision itself."*

The Court further observed that, this analysis was squarely applicable to lection 85 of the IT Act. On the grounds that the company was not arraigned as n accused in the *Baazee*case, the proceedings against the petitioner were

Concept of Corporate Criminal Liability in India: Legally, a company is considered to be a person and therefore, criminal liability is imposed on it. However, difficulties arise with this, especially in the case of offences where m*ens rea* is an essential ingredient, or where punishment in the form of imprisonment is mandatory. For example, currently the IT Act:

(i) Sections 66A, 66C, 66D, 67, 67A, 67B, 67C, 69, 69A, 69B and 70 of the IT Act prescribe imprisonment and fine.

(ii) Section 66F of the IT Act prescribes imprisonment only.

(iii) Sections like 65, 66E, 66F, 67C, 68, 69B and 74 of the IT Act specifically require an element of *mensrea, i.e.,* the offences should have been done intentionally or knowingly

Proving the 'guilty mind' of a corporation or imprisoning it is not possible. The stand taken by Indian courts on the criminal liability of companies has been varying greatly:

(i) ***1974: Company cannot be prosecuted for an offence where mensrea is an essential ingredient:*** **In** the **case of *Champa*** *Agency v. R. Chowdhury:*

> *"...mensrea is an essential ingredient of the offence of criminal breach of trust including criminal breach of trust by carriers. The accused... being a corporate body cannot be said to have the necessary mensrea and as such it cannot be prosecuted for an offence under Section 407 of the Indian Penal Code."*

(ii) ***1987: Company cannot be prosecuted for an offence where imprisonment is mandatory:*** **In** the case of *Adding Machines India (P) Ltd.* v. *State:*

> *"...in respect of offence where the sentence prescribed is mandatory imprisonment and the court has no discretion to impose any other punishment, such as fine, a company cannot be prosecuted in respect of such an offence."*

(iii) ***1997: Only a fine can be imposed on a company for an offence where imprisonment and fine are mandatory:*** **In** the case of *M.V. Javali v. Mahajan Borewell & Co. and Ors:*

> *"... the mandatory sentence of imprisonment and fine is to be imposed where it can be imposed, namely on persons coming under categories (ii) and (iii) above, but where it cannot be imposed, namely on a company, fine will be the only punishment."*

(iv) ***2004: No choice to impose only a fine on a company for an offence where imprisonment and fine are mandatory:*** In the case of *The Assistant Commissioner, Assessment-II, Bangalore &Ors.* v. *VelliappQ Textile,* the Supreme Court overruled the position taken in M.V. Javali:

> *"Where the legislature has granted discretion to the court in the matter of sentencing, it is open to the court to use its discretion. Where, however, the legislature, for reasons of policy, has done away with this discretion, it is not open to the court to impose only*

> *a part of the sentence prescribed by the legislature, for that would amount re-writing the provisions of the statute."*

(v) ***2005: No immunity to companies from prosecution for offences where mandatory imprisonment is prescribed:*** **In the** case of *Standard Chartered Bank and Ors. v. Directorate of Enforcement*[67]*:*

> *"...there could be no objection to a company being prosecuted for penal offences ... and the fact that a sentence of imprisonment and fine has to be imposed and no imprisonment can be imposed on a company or an incorporated body, would not make Section ... inapplicable and that a company did not enjoy any immunity from prosecution in respect of offences for which a mandatory punishment of imprisonment is prescribed."*

(vi) ***2011: Mensrea is attributed to companies on the principle of alter ego' of the company:*** The case of *Iridium India Telecom* ***Ltd*** *v. Motorola Inc.* lays down the following position on the imposition of criminal liability on companies:

> *"...a corporation is virtually in the same position as any individual and may be convicted of common law as well as statutory offences including those requiring mensrea. The criminal liability of a corporation would arise when an offence is committed in relation to the business of the corporation by a person or body of persons in control of its affairs. In such circumstances, it would be necessary to ascertain that the degree and control of the person or body of persons is so intense that a corporation may be said to think and act through the person or the body of persons. ... Mensrea is attributed to corporations on the principle of "alter ego' of the company."*

Miscellaneous Provisions

Section 77 - Compensation, penalties or confiscation not to interfere with other punishment: Section 77 of the IT Act reads as follows:

> *"No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force."*

Any penalty, compensation or confiscation awarded under this Act will be independent of the award of any other penalty or punishment under any other law for the time being in force. This section essentially prevents the use of the plea of double jeopardy or *autre fois convict*[69]on the grounds of a conviction under this Act.

Section 77 A - Compounding of Offences: Section 77A of the IT Act reads as follows:

> *"(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.*
>
> *Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.*
>
> *Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.*
>
> *(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply."*

This section lays down when an offence cannot be compounded:

(i) An offence with a term of imprisonment exceeding 3 years, or with punishment of life.

(ii) Any offence where the accused is liable to enhanced or different punishment on account of a previous conviction.

(iii) Any offence which affects the socio-economic conditions of the country.

(iv) Any offence which affects a child below the age of 18 years or a woman.

The application for compounding can be filed by the accused in the same court where his offence is to be or being tried. The provisions of Criminal Procedure Code with respect to plea bargaining, *i.e.,* Section 265 B, Application for Plea bargaining and Section 265C, Guidelines for Mutually Satisfactory Disposition, will be applicable to the filing of this application.

Section 77 B - Offences with 3 years' Imprisonment to be Cognizable:

Section 77B of the IT Act reads as follows:

> *"Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable."*

Offences punishable with imprisonment of 3 years and above are cognizable, while, offences with a punishment of less than 3 years are non- cognizable. Offences punishable with imprisonment of 3 years and below are bailable, while, offences with more than 3 years are non-bailable.

Section 63 - Compounding of Contraventions: Section 63 of the IT Act reads as follows:

> *"(1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:*
>
> *Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.*

(2)Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3)Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded."

This section provides a Controller or Adjudicatory officer or anyone authorised for this purpose by them with the power to compound contraventions. The rules for compounding **are:**

(i) Penalty should not exceed maximum penalty prescribed.

(ii) A second commission of the same or similar contravention within 3 years from the first commission cannot be compounded.

(iii) Once a contravention is compounded, no proceeding or further proceeding may be taken against the person.

Comparison of Cognizability, Bailability and Compoundability of Offences and Contraventions under the IT Act

Contravention / Offence	**Imprisonment**	**Cognizability**	**Bail ability**	**Compound ability**
43-Damage to computer, Computer system or computer	Damages (no limit)	Not Applicable	Not Applicable	Compoundable
65-Tampering with computer source documents	Upto 3 yrs/ Fine Rupees 2L/ both	Cognizable	Bailable	Compoundable

66-Computer Related offences	Upto 3 yrs/ Fine Rupees5L/ both	Cognizable	Bailable	Compoundable
66A-Sending offensive messages through communication service	3 yrs and Fine	Cognizable	Bailable	Compoundable
66B-Dishonestly receiving stolen computer resource or communication device	Upto 3 yrs/ Fine Rupees1L/ both	Cognizable	Bailable	Compoundable
66C-Identity theft	Upto 3 yrs/ Fine Rupees1L/ both	Cognizable	Bailable	Compoundable
66D-Cheatingby personation by using computer resource	Upto 3 yrs and Fine Rupees 1L	Cognizable	Bailable	Compoundable
66E-Violation of privacy	Upto 3 yrs/ Fine Rupees2L/ both	Cognizable	Bailable	Compoundable
66F-Cyber Terrorism	Upto life imprisonment	Cognizable	Non-Bailable	Non-Compoundable
67-Publishing or transmitting obscene material	1stConviction: Upto 3 yrs and Fine Rupees 5L 2nd Conviction: Upto 5 yrs and Fine Rupees 10L	Cognizable	Non-bailable	Non-Compoundable on 2nd Conviction
67A-Publishingor transmitting of material containing sexually explicit act, *etc.* in electronic form	IstConviction: Upto 5 yrs and Fine Rupees 10L 2nd Conviction: Upto 7 yrs and Fine Rupees 10L	Cognizable	Non-bailable	Non-Compoundable

67B-Publishingor transmitting of material depicting children in sexually explicit act, *etc.*in electronic form	1slConviction: Upto 5 yrs and Fine Rupees 10L 2nd Conviction: Upto 7 yrs and Fine Rupees 10L	Cognizable	Non-bailable	Non-Compoundable
67C-Non-compliance with the directions of the government for	Upto 3 yrs and Fine	Non-cognizable	Bailable	Compoundable
preservation and Retention of information by intermediaries				
68-Failure to comply with the directions issued through an order of the Controller under section 68	Upto 2 yrs/ Fine Rupees1L/ both	Non-cognizable	Bailable	Compoundable
69-Failure to assist agency in intercepting or monitoring or decrypting any information through any computer source.	Upto 7 yrs and Fine	Cognizable	Non-bailable	Non-Compoundable
69A-Failure to comply with directions for blocking of public access of any information through any computer resource	Upto 7 yrs and Fine	Cognizable	Non-bailable	Non-Compoundable

69B-Failureof intermediary to assist agency appointed by the government to monitor and collect traffic data or information through any computer resource for cyber security.	Upto 3 yrs and Fine	Cognizable	Bailable	Compoundable
71-Penalty for misrepresentation	Upto 2 yrs/ Fine Rupees1L/ both	Non-cognizable	Bailable	Non-Compoundable
72-Penalty for breach of confidentiality and privacy	Upto 2 yrs and Fine Rupees 1L	Non-cognizable	Bailable	Compoundable
72A-Punishment for disclosure of information in	Upto 3 yrs/ Fine Rupees5L/ both	Non-cognizable	Bailable	Non-Compoundable
Breach of lawful contract				
73-Penalty for publishing Electronic Signature Certificate false in certain particulars	Upto 2 yrs/ Fine Rupees IL/ both	Non-cognizable	Bailable	Compoundable
74-Publication for fraudulent purpose	Upto 2 yrs/ Fine Rupees 1L/ both	Non-cognizable	Bailable	Compoundable

Section 84 B - Punishment for abetment of offences: Section 84B of the IT Act reads as follows:

> *"Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for*

the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment. "

Under this section, the abetment of an offence shall be punishable with the same punishment as that provided for the offence, provided that:

(i) The offence that is abetted is actually committed as a result of the abetment. The explanation to the section provides that the act should be the result of the instigation, conspiracy or aid that constitutes the abetment. This explanation is similar to that provided under Abetment under the IPC.

(ii) The abetment of that offence has not been otherwise expressly provided for **under** the IT Act. For example, Section 43(g) of the IT Act expressly provides for a person who aids unauthorised access of a computer.

Section 84 C - Punishment for attempt to commit offences: Section 84B of the IT Act reads as follows:

"Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both."

Under this section, when a person attempting or causing the commission of an offence does an act towards the commission of the offence, he shall be punishable with the half of the longest term of imprisonment or half of the fine as provided for the offence. This is provided that the attempt of that offence has not been otherwise expressly provided for under the IT Act. For example, Section 70 of the IT Act specifically provides for an attempt to access a protected system.

ADJUDICATION UNDER THE IT ACT

Cyber Appellate Tribunal

The Cyber Appellate Tribunal (the "CAT") is established by the Central Government to hear and adjudicate appeals against the orders of the Controllers or Adjudicating Officers. The provisions applicable to the CAT are laid down under Chapter X of the IT Act:

(ii) **Composition of CAT:** The Central Government on consultation with the Chief Justice of India appoints a Chairperson of the CAT to preside over the proceedings brought before the tribunal and such number of other Members as specified.

(iii) **Powers of Chairperson:** The Chairperson, formerly known as the Presiding Officer (prior to amendment), has the powers of general superintendence and directions over the affairs of the CAT and such other powers and functions as may be prescribed, in addition to the power to preside over the proceedings. The Chairperson may also distribute matters among the Benches of the CAT, and also transfer matters before them either on application or *suomoto*without notice[77]. In case of a difference in opinion between two Members of a Bench, the matter may be referred to the Chairperson. Such disputes are to be decided in accordance with the majority opinion of the Members who have heard the case.

(iv) **Appeal from Orders of Controller or Adjudicatory Officers:** Any person aggrieved by an order of a Controller or Adjudicatory officer may appeal to the CAT having jurisdiction in the matter within 45 days of receiving the order. However, no appeal will lie from orders given with the consent of the people. The CAT shall dispose of such appeals expeditiously, and shall endeavour to dispose of it finally within 6 months of receipt.

In the case of *Dr. Avinash Agnihotri v. Controller of Certifying Authorities and Others* before the Cyber Appellate Tribunal, it was held that without exhausting the alternative remedy of approaching the Adjudicating Officer appointed under the IT Act, no appeal is maintainable before the CAT.

(iv) **Procedure of CPC not Applicable:** The procedure laid down by the Code of Civil Procedure, 1908, is not applicable to the CAT. It is, however, to be guided by the principles of natural justice.

(v) **Power to regulate its Procedure:** The CAT has the powers to regulate its own procedure including the place at which it would hear the matters before it.

(vi) **Powers of a Civil Court:** The CAT has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, for the purposes of discharging its functions under the IT Act in respect of the following matters:

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte

(g) any other matter which may be prescribed.

(vii) **Proceedings Deemed to be Judicial Proceedings:** Proceedings before the CAT are deemed to be a judicial proceeding within the meaning of Sections 193 (Punishment for false evidence) and 228 (Intentional insult or interruption to public servant sitting in judicial proceeding) of the IPC and for all the purposes mentioned under section 196 (Using evidence known to be false) of the IPC, meaning that the CAT has the power to punish for furnishing false evidence and intentionally insulting or interrupting any public servant during judicial proceedings .

(viii) **CAT Deemed to be a Civil Court for Certain Purposes:** The CAT is deemed to be a civil court for the purposes mentioned in section 195 (which lists offences which the court may not take cognizance of unless the conditions provided therein are satisfied) and Chapter XXVI of the Code of Criminal Procedure, 1973 (Provisions as to offences affecting the administration of justice).

(ix) **Provisions of Limitation Act:** As the CAT enjoys the powers of a judicial court, hence, as per section 60 of the Act, the provisions of the Limitation Act, 1963, have been made applicable to the proceedings of the CAT.

(x) **Civil Court not to Have Jurisdiction:** No civil court shall have a jurisdiction to entertain a suit or proceeding, or grant an injunction over a matter in respect of which the CAT or Adjudicatory Officers have jurisdiction. However, a Court may exercise jurisdiction over a claim for injury or damage that exceeds the maximum amount which can be awarded under this Chapter

(xi) **Appeal to High Court:** Any appeal on any question of fact or law arising in a decision of the CAT lies with the High Court of the concerned state within 60 days of the date of communication of the decision. The High Court may extend the period of filing an appeal by another 60 days for sufficient cause.

Certain rules have been laid out by the Central Government in exercise of its powers under Section 87 of the IT Act:

(i) Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000

(ii) Cyber Regulations Appellate Tribunal (Salaries, Allowances and Other Conditions of Service of other Officers and Employees) Rules, 2002

(iii) IT (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules, 2003

(iv) Cyber Appellate Tribunal (Salaries, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009

(v) Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour and/or Incapacity of Chairperson and Members) Rules, 2009

Adjudicatory Officers

The IT Act provides for appointment of an Adjudicating Officer by the Central Government for inquiring into and adjudicating contraventions under the Act under Sections 46 and 47 of the IT Act:

(i) **Jurisdiction:** The appointment of an Adjudicating Officer is for the purpose of adjudicating, if, any person has contravened any provisions of the Act. The Adjudicating Officers can exercise the jurisdiction only with respect to contraventions mentioned under Chapter IX of the Act, *i.e.,* Sections 43, 44 and 45 of the IT Act. If during the hearing or investigation of a matter, the Adjudicating Officer is convinced that the scope of matter falls under Chapter XI of the Act, he must transfer the case to the Magistrate with jurisdiction to entertain the matter. The Adjudicating Officer also has the power to take *suomotu* cognizance of any matter.

In the case of *S. Sekarv. The Principal General Manager,* the petitioner was prosecuted under Sections 406, 420 and 468 of the IPC and Section 43(g) of the IT Act for offences committed by the manipulations of a computer system. The Madras High Court held that it did not have the jurisdiction to hear a matter which involved a criminal charge under Section 43(g) of the IT Act. This jurisdiction had been expressly vested in the Adjudicatory Officer under Section 46(1) of the IT Act.

(ii) **Pecuniary Jurisdiction:** The Adjudicatory Officer is empowered to adjudicate the cases where the claim for injury or damage does not exceed Rupees 5 Crore. In cases where the claim exceeds this amount, the jurisdiction will lie with the competent court.

(iii) **Powers of a Civil Court:** Every Adjudicatory Officer shall have the powers of a civil court which are vested in the CAT under Section 58(2).

(iv) For the purposes of section 193 and 228 of the IPC, the proceedings before an Adjudicating Officer are considered to be judicial proceedings.

(v) The Adjudicatory Officer will be deemed to be civil court for the purpose of Sections 345 (Procedure in cases of contempt), 346 (Procedure when Court thinks that the case should not be dealt under Section 345) and Order XXI (Power to try summarily) of the Code of Criminal Procedure[1].

(vi) The Adjudicating Officer while adjudging the quantum of compensation is required to take the following factors into account:

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default[2].

GENERAL TYPES OF CYBER-CRIMES

A brief description of various crimes that can be committed in cyberspace and the sections of the IT Act which are generally applicable to them are given below:

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
1	Bluetooth related crimes, such as Bluesnarfing (unauthorised access of information on a Bluetooth enabled device, such as a laptop, phone, *etc.)* and Bluejacking (sending of messages through Bluetooth enabled devices)	Same as Hacking (No. 25 of this Table) Section 66A (Sending offensive message through communication service)		
2	Child Pornography (viewing, downloading, creation, publication, transmission, downloading, exchange, *etc.)*	Section 67-B (Punishment for publication or transmission of material depicting children in sexually explicit act, *etc.* in electronic form)	Section 292 (Sale, *etc.* of obscene books, *etc.)* Section 293 (Sale *etc.* of obscene objects to young person) Section 294 (Obscene acts and songs)	Section 11, (Sexual Harassment) and Section 13, (Use of a child for pornographic purposes), of Protection of Children from Sexual Offences Act, 2012
3	Computer Source Code related crimes (Alteration, deletion, damage, theft, *etc.*	Section 43(j) (Theft of computer source code)		Section 63B (Knowing use of infringing copy of
	Example - Alteration of computer source code of a cell phone)	Section 65 (Tampering with computer source code		computer programme) of Copyright Act, 1957"

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
4	Copyright Infringement including Abetment of Copyright Infringement (Unauthorised online reproduction, publication, use, *etc.* of documents, photographs, literary works, software, music, videos, *etc.* Example - Infringing use of copyrighted user interface of a software program.	Section 43 (b) (Unauthorised download/ copying/ extraction of data) Section 66 (Computer related offences)		Section 51 (Infringement of copyright) and Section 63 (Punishment for offence of infringement) and Section 63B (Knowing use of infringing copy of computer programme) of Copyright Act, 1957
5	Credit Card and Related Frauds (Extraction of credit card information like usernames and passwords and their use for financial frauds. Extraction of information may be through hacking, phishing, viruses **like** keyloggers, *etc.)*	Section 43(a) (Unauthorised Access) Section 43 (b) (Unauthorised download/ copying/ extraction of data) Section 43 (c) (Introduction of computer contaminant /virus) Section 43(i) (Destruction of Information in a Computer Resource) Section 66 (Computer related offences) Section 66A(c) (E-mails sent to		

Sl.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
		deceive/ mislead as to origin) Section 66C (Identity Theft) Section 66D (Cheating by Personation)		
6.	Cyber Bullying (Bullying of a person through the internet in a deliberate and repeated manner. Methods may include publication of defamatory matter, hacking into the persons' accounts, online stalking and creation of fake accounts in the person's name)	Section 66-A (Punishment for sending offensive messages through communication service) Section 67 (Publication of obscene material in electronic form) Same as Cyber Defamation (No.7), Hacking (No.40), Identity Theft (No.26)		
7.	Cyber Defamation (Online defamation, for example - Defamatory messages sent via e-mail, Defamatory articles published online)	Section 66A (Punishment for sending offensive messages through communication service) Section 67 (Publication of obscene material in electronic form)	Section 499 (Defamation) Section 469 (Forgery of electronic record for the purpose of harming reputation)	

8	Cyber Espionage (Use of computer resource for obtaining secret and confidential information from another person, such as a rival business, enemy nation, *etc.* Methods of obtaining information include hacking and use of malicious software)	Same as Hacking (No.40) and Virus Attacks (No.49) Section 66F (Cyber terrorism)		
9	Cyber Harassment (A more serious form of cyber bullying)	Same as Cyber Bullying (No.6)		
10	Cyber Squatting (Registration or acquisition of website, or domain name, that is identical to another's trademark, with the intention of selling it to the trademark holder at a higher price or diverting the customers of the trademark holder, *etc.)*			Section 27 (Passing off) and Section 29 (Infringement of registered trademarks) of Trademarks Act, 1999
11	Cyber Stalking (Online stalking or harassment of a person. Means include monitoring online activites of a person such as e-mail usage through hacking and introduction of viruses, identity theft, online defamation and online intimidation)	Same as Cyber Bullying (No.6)	Section 354-D (D(ii) (Monitoring use by a woman of internet, e-mail or other electronic communication)	

12	Cyber Terrorism (Internet based terrorist activities. Means include unauthorised access of highly confidential data, denial of service attacks , disruption of critical infrastructure systems or large scale disruptions of computer systems)	Section 66-F (Punishment for cyber terrorism)		
13	Cyber Threatening (Threatening of a person through the internet, for example - sending of threatening e-mails)	Section 66A (a) and (b) (Punishment for sending offensive messages through communication service)	Section 503 (Criminal Intimidation)	
14	Cyber Warfare (War between nations carried out through online means, for example - through large scale hacking of computer systems, denial of service attacks, cyberterrorism, cyber espionage)	Section 66F (Cyber Terrorism)		
15	Data Diddling/ False Data Entry (Involves unauthorised and insignificant alterations to data, usually before it is entered into a computer system, resulting in a false representation of the data. Example - Diversion of goods to criminals through changes made to delivery addresses while processing orders from clients)	Section 43 (a) (Unauthorised Access) Section 43 (d) (Damage to data, computer database, *etc.)* Section 66 (Computer Related Offences)	Section 463 (Forgery) Section 464 (Making false electronic record) Section 468 (Forgery for the purpose of cheating)	

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
16	Denial of Service Attacks and Distributed Denial of Service Attacks (Attack by overloading a website or network with requests, making the website unavailable for regular users. A distributed denial of service attack involves requests being sent from several computers, which are known as a 'botnet'. Thebotnetis created through the introduction of viruses in others' computers without their knowledge. May be used as a form of cyber terrorism, to disrupt the business of a rival, as a form of cyber threatening, *etc.)*	Section 43 (a) (Unauthorised Access) Section 43 (c) (Introduction of computer contaminant /virus) Section 43 (d) (Damaging Computer) Section 43(e) (Disruption of Computer) Section 43(f) (Denial of access) Section 43 (i) (Destruction of Information) Section 66(Computer Related Offences) Section 66F(l)(A)(i) (Cyber Terrorism using a denial of service attack)		
17	Digital Signature Certificates and related crimes	Section 73(Publication of false electronic signature certificate) Section 74 (Creation or publication of false electronic signature)	Section 464 (Creation of false electronic record through dishonest/ fraudulent affixation of electronic signature)	
18	Disclosure of sensitive and personal information	Section 43A (Compensation for failure to protect data) Section 72 (Breach of Confidentiality and Privacy)		

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc.
19	Dishonestly receiving stolen computer, computer system, computer network, data, computer data base or software (For eg- Accepting stolen laptop, usage of pirated software, *etc.)*	Section 66B (Dishonestly receiving stolen computer resource or communication device)	Section 411 (Dishonestly receiving stolen property)	
20	E-mail Bombing (Form of denial of service attack involving the flooding of an e-mail address with huge volumes of e-mails. May be in the form of sending duplicate mails to the same e-mail address, signing up the e-mail address for several subscriptions, *etc.)*	Section 43 (a) (Unauthorised Access) Section 43(e) (Disruption of Computer) Section 43(f) (Denial of access) Section 66(Computer Related Offences) Section 66A(c) (Sending of e-mail for causing annoyance/ inconvenience) Section 66E (Identity Theft)		
21	Email Scams (A form of cyber fraud involving the sending of unsolicited e-mails for fraudulent purposes. Example - The Nigerian scam, where the e-mail promises a percentage of money claimed to have been won or received in an inheritance on payment of an advance fee, Online dating scams, *etc.)*	Section 66A(c) (Sending of e-mail to deceive as to origin) Section 66D (Cheating by personation)	Section 415 (Cheating)	

Sl, No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
22	E-mail Spam (Sending of bulk unsolicited e-mails, usually involving the sending of the same mail to several recipients. Opening the mail may lead the recipient to a fraudulent website or result in the introduction of a virus)	Section 66A(c) (Sending of e-mail for causing annoyance, or inconvenience, or to deceive as to origin)		
23	E-mail Spoofing (Form of e-mail scam where the e-mail consists of a forged e-mail address so it appears to be from someone else. Example - An e-mail purporting to be from State Bank of India from 'xyz@sbi.com' where the actual address of State Bank of India is 'xyz@statebankofindia.com'	Section 66A(c) (Sending of e-mail to deceive as to origin) Section 66D (Cheating by personation)	Section 415 (Cheating) Section. 416 (Cheating by personation)	
24	Forgery of electronic records and related crimes		Section 464 (Making of electronic records) Section 466 (Forgery of electronic record of a Court, public register, *etc.)* Section 468 (Forgery of electronic record for the purpose of cheating)	

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
			Section 471 (Knowing use of a forged electronic record as genuine.) Section 474(Knowing possession of a forged electronic record with intention of using it as genuine.) Section 476 (Counterfeiting device or mark used for authenticating electronic records or	
25	Hacking (Unauthorised access of a computer resource through the exploitation of some weakness in the security system, or through the insertion of a virus, password cracking, or any other means)	Section 43(a) (Unauthorised Access) Section 43(b) (Downloading/ Extracting Data) Section 43(c) (Introduction of a Computer Contaminant/ Virus) Section 43(d) (Damaging a Computer) Section 43(e) (Disrupting a Computer) Section 43(f) (Denying Access) Section 43(i) (Destruction of Information in a		

Sl. No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc.
		(Computer Related Offences)		
26	Identity theft (Involves the stealing of a person's online identity. May be used for extraction of information, financial fraud such as credit card fraud or conduct of criminal activities in the name of the person)	Section 66C (Identity Theft)		
27	Internet Time Theft (Involves usage of internet hours that have been paid for by another person)	Section 43 (h), (charging of services availed by one person to the account of another person by manipulating computer/ computer system/ network)		
28	Logic Bomb (A form of malware where a portion of the software code has been programmed so as to perform damaging acts on fulfilment of certain specified conditions without the knowledge of the user of the software. Example - A logic bomb set to activate on a certain date and wipe the hard drive of a computer)	Same as Malware (No.29)		

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
29	Malware (Malicious software, or a form of a virus that performs malicious activities, such as data theft, theft of confidential data, disruption of computer system or network, *etc.)*	Section 43(b) (Downloading/ Extracting Data) Section 43(c) (Introduction of a Computer Contaminant/ Virus) Section 43(d) 'Damaging a Computer) Section 43(e) (Disrupting a Computer) Section 43(f) (Denying Access) Section 43(i) (Destruction of Information in a Computer Resource) Section 66 (Computer Related Offences)		
30.	Money Laundering on Web (Online money laundering. Example - Maintaining a web service for the collection of illegal money obtained through activities like extortion and tax evasion)			Section 3 and 4 of the Prevention Of Money Laundering Act, 2002. (Offence and punishment for money laundering)
31	Music piracy (unauthorised downloading, sharing, copying, distribution, *etc.,*	Same as Copyright Infringement (No. 4)		

32	Net extortion (The use of the internet for coercively obtaining money, property, illegally *etc.* Means of extortion include threat of disclosure of confidential data, cyber defamation, cyber threatening and denial of	Section 66A (a) and (b) (Punishment for sending of offensive message through communication service) Various other		Sections 420, 465,471,474
33	Obscene or offensive content (Online publication, distribution, transmission, *etc.)*	Section 66A (Sending of offensive message through communication service) Section 66E (Violation of privacy) Section 67 (Publication/ transmission of obscene information in electronic form)Section 67 A Publication/transmission of Material containing sexually explicit act)Section 67B (Child Pornography)	Section 292 (Sale, *etc.* of obscene books, *etc.)* Section 293 (Sale *etc.* of obscene objects to young person) Section 294 (Obscene acts and songs)	
34	Offences by Companies	Section 43A .(Failure to protect data) Section 85 (Offences by companies) Various other sections depending on the offence		Various sections of the Companies Act, 2013 depending on the offence

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
35	Online Drug Trafficking			Narcotic Drugs and Psychotropic Substances Act, 1885
36	Online Gambling			Public Gambling Act, 1867 Sikkim Online Gambling (Regulation) Act, 2009
37	Online Sale of Arms			Indian Arms Act, 1959
38	Patent Infringement (For example - Suits by Fotomedia against several entities including Yahoo! Inc, Photobucket.com, Fujifilm USA, Inc. for unlicensed use of patented photosharing software)			Patents Act, 1970

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
39	Pedophilia (Sexual abuse of children by adults through the internet)	Section 67-B (c) and (d) (Puni ,hment for publication or transmission of material depicting children in sexually explicit act, *etc.* in electronic form)	Section 293 (Sale *etc.* of obscene objects to young person)	Section 11, (Sexual Harassment) and Section 13, (Use of a child for pornographic purposes), of Protection of Children from Sexual Offences Act, 2012
40	Phishing (Extraction of sensitive information like usernames and passwords for the commission of financial fraud, by imitating a trustworthy source such as a bank, credit card company, *etc.* May be in the form of fake bank website, spoofed e-mails, personation, identity theft, *etc.*	Section 66A (c) (Sending E-mail to Deceive Recipient as to Origin) Section 66C (Cheating by Personation) Section 66D (Identity Theft)	Section 4l5(Cheating), 416 (Cheating by personation) Section 468 (Forgery for the purpose of cheating)	Section 27 (Passing off) and Section 29 (Infringement of registered trademarks) of Trademarks Act, 1999[10]
41	Pornography (Online publication or transmission)	Section 67A (Publication or transmission of material containing sexually explicit act, *etc.* in electronic form)	Section 292 (Sale, *etc.* of obscene books, *etc.)* Section 294 (Obscene acts and songs)	

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
42	Salami Attack (Involves unauthorised and insignificant alterations to data which results in an overall major financial fraud. Example - A person with access to the database of a bank's customers transfers a very small amount of money from every account every month into another account. The small deductions may go unnoticed by the customers, but on the whole a large amount is transferred to the illegal account.) Misappropriation of funds through changes made to company's accounts, *etc.*	Section 43 (a) (Unauthorised Access) Section 43 (d) (Damage to data, computer database, *etc.)* Section 66 (Computer Related Offences)	Section 463 (Forgery) Section 464 (Making false electronic record) Section 468 (Forgery for the purpose of cheating)	
43	Software Piracy	Same as Copyright Infringement (No.4) Section 66B (Dishonestly receiving stolen computer resource)		

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
44	Theft of Data (Unauthorised extraction, downloading or copying of confidential information, sensitive and personal information, other data or databases.)	Section 43 (a) (Unauthorised Access) Section 43 (b) (Unauthorised downloading/ copying/ extraction of data) Section 43-A (compensation for failure to protect data) Section 66 (Computer Related Offences) Section 66B Dishonestly receiving stolen computer resource) Section 72 (Breach of Confidentiality and Privacy) Section 72A (Disclosure of information in breach of lawful contract)		
45	Time Bomb (Form of software program that is programmed to stop functioning at a pre-determined time. Example - Use of a time bomb for industrial sabotage, by causing a critical software to stop functioning)	Same as Virus (No. 49)		

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
46	Trademark Infringement (Example - Cybersquatting, typosquatting, reverse domain name hijacking, trademark infringement through metatags, framing and linking)			Trademarks Act, 1999
47	Trojan (A software program that appears to be innocent but performs malicious function without the knowledge of the person using the software)	Same as Virus (No. 49)		
48	Video voyeurism and violation of privacy (Use of a camera, video recorder, *etc.* to capture or record images in circumstances violating a person's privacy)	Section 66-E (Punishment for violation of privacy)	Section 354-C (Voyeurism)	
49	Virus (Kind of computer program or software that destroys, damages or otherwise injuriously affects a computer resource)	Section 43 (c) (Introduction of Contaminant/ Computer Virus) Section 43 (d) (Damaging a Computer) Section 43 (e) (Disrupting a Computer) Section 43 (f) (Denying Access)		

S.No.	Cyber-crime	Sections under IT Act	Sections under IPC	Sections under Misc. Laws
		Section 43 (i) (Destruction of Information in a Computer Resource) Section 66 (Computer Related Offences)		
50	Web Defacement (Attack on website involving alteration of its visual appearance Example - Defacement of government websites by hackers)	Section 43(a) (Unauthorised Access) Section 43(i) (Destruction of Information in a computer resourcesComputer Resource) Section 66 (Computer Related Offences		

UNIT -4

INTELLECTUAL PROPERTY RIGHTS AND CYBERSPACE

Concept of Property in Cyberspace

Property, in terms of economic theory, is a valuable resource, and how this resource is put to use needs to be determined by an exclusive authority. The ownership of property, whether by the government or by individuals, comes with a 'bundle of legal rights', i.e., the right of possession of the property, right of control over the use of the property, right of excluding others from using or entering the property, right of enjoying the property in any manner which is legal and the right to transfer, sell, lease or otherwise dispose of the property at the owner's will. All such rights which vest in the owner are collectively known as property rights. These rights provide definite and enforceable rules for the community with respect to the access to and use of the benefits arising from property.

In the virtual world of cyberspace, the objects present are not in a tangible form like land is, but, are instead in the intangible form of digital information. Information available in cyberspace in the form of computer software, trade secrets, literary works like writings, novels and journals, creative works like paintings, photographs and sound recordings, etc. constitutes a valuable resource for their creator. However, this wealth of digital information contained in cyberspace is subject to a big risk which can be easily misused. The ease with which digital information can be created and disseminated implies that it can just as easily be accessed, used and modified without the knowledge of its owner. The result of this is that digital information also needs to be made the subject of property rights, and its use and access needs to be restricted.

Digital information, in terms of property, usually constitutes intellectual property, which is a creation of the mind, such as inventions; literary and artistic works; and symbols, names and images used in commerce. Digital information is therefore subject to intellectual property rights.

Agreement on Trade-Related Aspects of Intellectual Property Rights STRIPS), 1994

The Agreement on Trade-Related Aspects of Intellectual Property Rights (the "TRIPS Agreement"), 1994, administered by the World Trade Organization (WTO), is a comprehensive multilateral international agreement relating to intellectual property rights such as trademarks, copyrights, geographical indications, industrial designs, trade secrets, etc.

The TRIPS Agreement sets down the minimum standards for the regulation of IPR, including the grant of rights to the owner of intellectual property, the requirements concerning enforceability under the national laws and the settlement of disputes and relevant remedies in case of infringement. Since, it lays down minimum standards, the member nations of the TRIPS Agreement are allowed to provide more extensive protection to IPRs.

1. **Important Features**: The three important features of the agreement are:

(i) **Standards:** Members are firstly required to provide minimum standards for the protection of IPRs. These standards have been established by imposing the obligation of meeting the requirements of the international treaties such as the Berne Convention and the Paris Convention. The substantive provisions of these conventions have been incorporated by reference. In addition, the TRIPS agreement imposes several obligations where these treaties were inadequate. The main elements of protection with respect to IPRs are:

(a) The subject matter to be protected,

(b) Rights to be conferred and permissible exceptions to these rights, and

(c) The minimum duration of protection.

(ii) **Enforcement:** Members are secondly required to ensure that the enforcement procedures specified in the TRIPS Agreement are available under their law for the effective enforcement of rights. The TRIPS Agreement specifies general obligations, civil and administrative procedures and remedies, provisional measures, special requirements related to border measures and criminal procedures.

(iii) **Dispute Settlement**: Disputes between members with respect to their obligations under the TRIPS Agreement are to be resolved by the WTO's dispute settlement procedures.

2. TRIPS Agreement and IT: The TRIPS Agreement has some specific provisions which are applicable to IPRs for IT:

(i) Patenting in any field of technology Article 27 states that patents are available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application. This provides for the grant of a patent in 'any field of technology' that is capable of industrial application. Thus, members are required to provide patents protection for all inventions, including in the field of IT, for example, for software.

(ii) Copyright to Computer Programs and Compilations of Data: Article 10 protects computer programs and compilations of data as literary works under the Berne Convention. Computer programs include programs whether in the source code or the object code. Copyright protection with respect to compilations of data applies to the selection or arrangement of content and not in the content in itself. In other words, it applies only to the form (and not the substance) of the data compilation.

Overview of Indian Law relating to IPR

India became a member of the WTO and the TRIPS Agreement in 1995. The following laws were enacted to lay down the minimum standards for protection of IPR, in fulfillment of India's obligations under the TRIPS Agreement:

(i) Copyright Act, 1957: This Act provides exclusive rights to use reproduce and publish copies of original literary, dramatic, artistic and musical works, sound recordings, films, broadcasts, etc. A copyright is valid for a period of 60 years.

(ii) Patents Act, 1970: This Act grants an exclusive right to prevent unauthorized use, production, sale and import with respect to an 'invention', i.e., a new product or process involving an inventive step and capable of industrial application. A patent is valid for a period of 20 years.

(iii) Trademarks Act, 1999: This Act protects a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours. A trademark is valid for a period of 10 years.

(iv) Geographical Indications of Goods (Registration and Protection)Act, 1999: This Act protects an indication which identifies goods like agricultural goods, natural goods or manufactured goods a shaving originated/ been manufactured from a particular territory. This right is granted when a given quality, reputation or other characteristic of such goods is essentially attributable to its geographical origin. This right exists for a period of 10 years.

(v) Designs Act, 2000: This Act gives an exclusive right over the features of shape, configuration, pattern, ornament or composition of lines or colours applied to any article whether in two dimensional or three dimensional or in both forms. The right exists in the form of a copyright for a period of 10 years.

(vi) Semiconductor Integrated Circuit layout Design Act, 2000: This Act protects a product having transistors and other circuitry elements which are inseparably formed on a semiconductor material or an insulating material or inside the semiconductor material and designed to perform an electronic circuitry function. This right exists for a period of 10 years.

(vii) Protection of Plant Varieties and Farmers' Rights Act, 2001: This Act protects the rights of plant breeders in order to stimulate investment for research and development of new plant varieties. The duration of this right varies based on the plant variety, for example, six years for crops, nine years for trees and so on. The maximum possible period including renewal is 18 years for trees.

ONLINE COPYRIGHT INFRINGEMENT

Online copyright infringement may occur with respect to any material that is copyrighted (and not computer programmes or computer generated works). For example, printing of copyrighted material can lead to the creation of unauthorized physical copies, while acts like scanning create unauthorized digital copies. Both acts amount to reproduction of the copyrighted work, which is the author's exclusive right and constitutes infringement. For example, Section 52 of the Indian Copyright Act, which is explained below, permits reproduction done only for the purposes of a judicial proceeding, for use by the Legislature or under a law for the time being in force. Reproduction for any other purpose would constitute infringement. Similarly, the posting of copyrighted material on a networking site will amount to unauthorized publication, another exclusive right of the author.

Law on Copyright in India

The Indian law on copyright, the Copyright Act was enacted in 1957. The Act is compliant with most international copyright conventions, including the Berne Convention, the Universal Copyright Convention and Articles 9 to 14 of TRIPS-The most recent amendments were made in 2012 specifically to bring India in line with the WIPO Copyright Treaty and the WIPO Performances and phonograms Treaty. In addition to these three treaties, India is also a signatory to the Geneva Convention for the Protection of rights of Producers of Phonograms.

Summary of Important Provisions of the Copyright Act, 1957: Section 14 of the Copyright Act, 1957 defines copyright as an exclusive right created by virtue of this Act to reproduce, publish, perform, produce, adapt or translate a literary, dramatic, musical or artistic work, or any cinematographic film, or a record. Under Section 13 of the Act, a copyright will not be provided for a work unless it was first published in India, or is by an Indian citizen or is located in India. The only exception provided to this rule is under Section 40 of the Act with respect to an international copyright.

Section 17 of the Act provides that the author of a work shall be the first owner of a copyright, and such author may assign or license the copyright to another person under Sections 18 and 30 of the Act respectively. The term of the copyright is provided for under Section 22-29 of the Act. For a literary, dramatic, musical or artistic work, the term is 60 years after the author's death, for anonymous and pseudonymous publications, photographs, cinematograph films and records, the term is 60 years from the date of publication, etc. The rights of copyright societies and broadcasting authorities and performers are also covered under this Act.

Sections 44 to 50 of the Act provide for registration of copyright and establish the Register of Copyrights. Registration is, however, not compulsory in India, and the protection under the Act applies equally to registered and unregistered copyright.

Under Section 51 of the Act, a copyright work will be infringed if any person does any of the acts which constitute an exclusive right of the author under Section 14 of the Act. If any person makes, sells, lets for hire, distributes, exhibits or imports copies of an author's work, he will also be liable for infringement. Several exceptions to this section have been provided under Section 52 of the Act, such as a fair dealing for the purpose of research, criticism, for reporting of current events (newspaper/ radio), reproduction for a judicial proceeding or in any work of the legislature or under the requirements of any law, the reading or reciting of a work in public and publication for any bona fide educational purposes. Chapter XII of the Act provides for civil remedies by way of injunction, damages, accounts and otherwise for copyright infringement, and Chapter XIII of the Act provides for criminal remedies.

International Copyrights

Chapter IX of the Copyright Act provides for the extension of the provisions of this Act to international copyrights. The Indian Government promulgated the International Copyright Order, 1999, for this purpose, and has extended the provisions of the Act to a work first made or published in the territory or by a citizen/ national, etc. of a country which is signatory to the Berne Convention, the Phonogram Convention, the Universal Copyright Convention and the World Trade Organization. The term of such as copyright will not be longer than that granted by the country of origin.

There are several provisions in the Copyright Act that are specific to computer programmes. These have been covered in detail in the next section.

Computer Software and Copyright

Copyrightable information in Software: Copyrightable information in software may include:

(i) Preparatory design materials, e.g. flowcharts, diagrams, specifications, form and report layouts, diagrams, specifications, form and reportlayouts, designs for screen displays, etc.;

(ii) Computer programmes (object code and source code) and other executable code;

(iii) Software development tools, e.g. Relational database development systems, compilers, report generators, etc.;

(iv) Information stored on computer media, e.g. conventional works such as literature, artistic works, music, etc. stored digitally;

(v) Database and data files;

(vi) Computer output e.g. Sound, print-out, computer file or data, electronic signals;

(vii) Screen displays;

(viii) Manuals and guides (on paper or stored digitally);

(ix) Programming languages.

Definition

Set of statement or instruction to be used directly or indirectly in a Computer to perform a particular task or to achieve a particular result.

Copyright Protection for Computer Programs:

- The nature of computer programs: primarily utilitarian, but protected as a literary work
- Copyright protection for computer programs can swathe copyrightable & non-copyrightable expressions within the continuum of ideas, expressions and algorithms
- Copyright protects only originality in expression. It extends to non-literal elements in a computer program. However, not all non-literal elements are protected expressions

Subject Matter of Copyright Protection;

- The Copyright Act 1957

Sec 13 Works in which Copyright subsist

(1) (a) original literary, dramatic, musical and artistic work;

(b) cinematograph films; and

(c) sound recording.

Minimum standard requirement for Copyright Protection:

- **Original**
- **Fixation**
- **Idea – Expression Dichotomy**
- **Art 9.2 TRIPs :** Copyright protection shall extend to *expression* and not to *ideas, procedures, method of operation or mathematical concepts*

Sec 2 (ffc)- Computer Programme:

- Computer programme means a set of instruction expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular results.

Elements in Computer Program-

➢ **Literal Elements (textual part)**

object code

source code

➢ **Non Literal Elements (functional part)**

Judicial interpretation of originality Concept (Literary work):

- University of London Press Ltd. v. University Tutorial Press Ltd.,(1916) 2 Ch 601

The word 'original' does not in this connection mean that the work must be the expression of original or inventive thought. Copyright Acts are not concerned with the originality of ideas, but with the expression of thought, and, in the case of 'literary work,' with the expression of thought in print or writing.

The originality which is required relates to the expression of the thought. But the Act does not require that the expression must be in an original or novel form, but that the work must not be copied from another work- that it should originate from the author.

"What is worth copying is, prima facie, worth protecting'

Feist Publication Inc. v. Rural Telephone Service Co. Inc., 499 US 340 (1991):

- Original, as the term is used in copyright, means only that the work was independently created by the authors (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity.
- Originality requires independent creation plus a modicum of creativity.
- Sweat of the Brow Doctrine – rejected

Fixation 17 USC Sec 101-

- A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.

Idea –Expression Dichotomy;

- Doctrine of Merger
- Baker v. Seldon 101 US 99 (1880).

The use of the art is a totally different thing from a publication of the book explaining it. In using the art, the ruled lines and headings of accounts must necessarily be used as incident to it.

Ratio…

- Whether the art might or might not have been patented is a question which is not before us. It was not patented, and is open and free to the use of the public. And of course, in using the art, the ruled lines and headings of accounts must necessarily be used as incident to it.
- The very object of publishing a book on science or the useful arts is to communicate to the world the useful knowledge which it contains. But this

object would be frustrated if the knowledge could not be used without incurring the guilt of piracy of the book. And where the art it teaches cannot be used without employing the methods and diagrams used to illustrate the book, or such as are similar to them, such methods and diagrams are to be considered as necessary incidents to the art, and given therewith to the public; not given for the purpose of publication in other works explanatory of the art, but for the purpose of practical application.

Anil Gupta v. Kunal Das Gupta (2002)25 PTC 1 (Del):

- An idea per se has no copyright. But if the idea is developed into a concept fledged with adequate details, then the same is capable of registration under the Copyright Act.
- R. G. Anand v. Delux Films (1978) 4 SCC 118.

Literal Element
Apple Computer Inc. v. Franklin Computer Corp (1983)-

- Whether copyright can exist in a computer program expressed in object code
- Whether copyright can exist in computer programme embedded on a ROM
- Whether copyright can exist in an operating system.
- Ratio- the copyright law protects the means of expressing an ideas and it is as near the whole truth as generalization can usually reach that if the same idea can be expressed in a plurality of totally different manners, a plurality of copyright may result.

Non- Literal Element
Whelan associates Inc. v. Jaslow Dental Laboratory Inc. and others (1986)-

- SSO
- Structure Sequence and Organization (Total look and feel)
- The purpose or function of a utilitarian work would be the work's idea, and everything that is not necessary to that purpose or function would be part of the expression of the idea. Where there are various means of achieving the

desired purpose, then the particular means chosen is not necessary to that purpose, hence there is an expression of idea. (End sought to be achieved).

Lotus Development Corp. v. Paperback Software international (1999)-

- Determining Copy right ability test laid down are

1. When the idea- expression distinction applies is to conceive and define the idea in a way that places it somewhere along the scale of abstraction
2. Whether an alleged expression of the idea is limited to elements essential to expression of that idea (or is one of only a few ways of expressing the idea) or instead includes identifiable elements of expression not essential to every expression of that idea.
3. Having identified elements of expression not essential to every expression of the idea, the decision maker must focus on whether those elements are a substantial part of the allegedly copyrightable work.

Computer Associates International Inc. v. Altai Inc. 982 F.2d 693 (3rdcir. 1992) –

- Abstraction.
- Filtration.
- Comparison.

Facts.... CA Scheduler

- t is an "operating system compatibility component" . It serve as a translator

AFC Test-

Abstraction test : reverse engineering – this process begins with the code and ends withand Adapter

- Zeke and Oscar 3.4 and Oscar 3.5
- CA Scheduler is a job scheduling program designed for IBM Frame
- Adapter is a program. I an articulation of the programs ultimate function

- **Filtration:** 1. Elements dictated by efficiency (Merger Doctrine)

  2. Elements Dictated by External factors –certain standard techniques has to be employed

a) The mechanical specifications of the computer on which a particular program is intended to run

b) b) compatibility requirement of other programs with which a program is designed to operate in conjunction

c) c) computer manufacturers' design standards

d) d) demands of the industry being serviced and

e) e) widely accepted programming practices within the computer industry.

3. Elements taken from public domain

f) **Comparison:** Golden nugget

Lotus Development Corp. v. Borland International (1995):

- Whether a computer menu command hierarchy is copyrightable subject matter.
- Lotus 123
- Quattro
- Lotus menu command hierarchy is not copyrightable because it is a system, method of operation, process or procedure foreclosed from protection by 17 USC Sec 102 (b).
- **17 USC Sec 102 (b)** - In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle or discovery, regardless of the form in which it is described, explained, illustrated or embodied in such work.
- The term method of operation refers to the means by which a person operates something, whether it be a car, a food processor or a computer. Thus a text describing how to operate something would not extend to copyright protection to the method of operation itself other people would be free to employ that method and to describe it in their own words. Similarly, if a new

method of operation is used rather than described, other people would still be free to employ or describe that method.

Right to make copies;

- MAI System Corp. v. Peak Computer Inc. (1993).
- The loading of copyrighted computer software from a storage medium (hard disk, floppy disk or read only memory) into the memory of a central processing unit (CPU) causes a copy to be made. The absence of ownership of the copyright or express permission by license, such acts constitute copyright infringement.
- Copy created in the RAM can be "perceived, reproduced or otherwise communicated". The court held that the loading of software into the RAM creates a copy under the Copyright Act.

Reverse Engineering of Computer Program Defined (Fair Use):

- Reverse engineering is defined as "starting with the known product and working backward to divine the process which aided in its development or manufacture"
- **Black box testing**
- **Decompilation- Computer** program are first written in a higher language known as source code. After that, it is translated into a form known as object code, a machine –readable form of 0's and 1's. Reverse engineering refers to the process of working backwards from the series of 0's and 1's to the higher language or source code. This copying of the object code for purposes of translating into source code has been referred to as "intermediate copying".

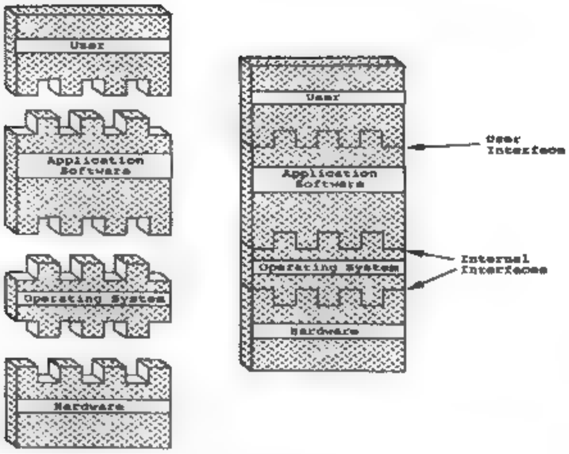
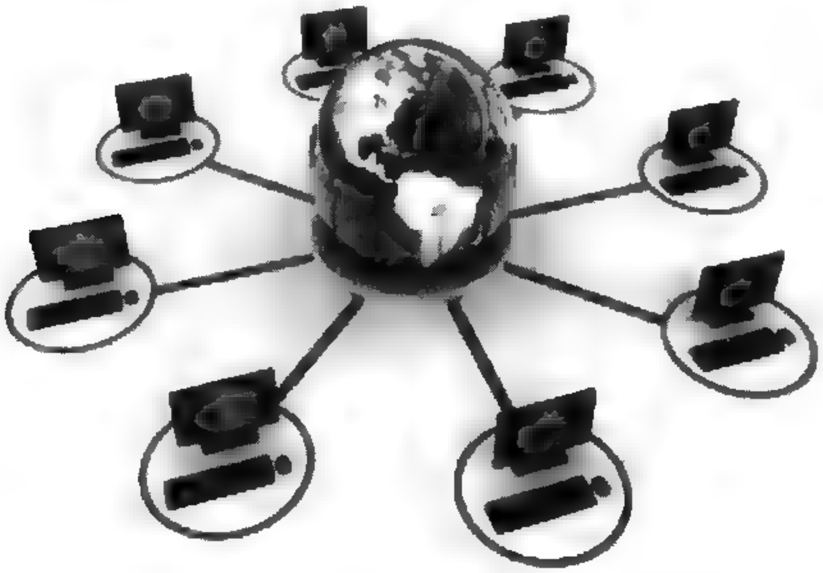


Figure -1: Compatible system

Network Externalities:

Interoperability (both vertical and horizontal) is a norm for innovation in software. It is by now widely accepted that interoperability is a fundamental to a competitive market framework for software products.



- Interoperability means the ability of computer programs to exchange information and of such programs mutually to use the information which has been exchanged.
- Horizontal Interoperability- Horizontal interoperability means the availability of interface information that allows the reverse engineer to develop his own operating system while being compatible with already existing application software. Software providers disclose interface specification of such quality and quantity as to enable subsequent software developers to analyze the interface information of the operating system necessary to develop independently their own operating system that is interoperable with other application programs. Therefore, horizontal interoperability leads to the development of independently created, competing operating systems which are compatible with other computer programs
- Vertical Interoperability- vertical interoperability software providers disclose interface information for their given operating system to application software providers to the extent to enable them to create new user programs independently.

17 U.S.C. § 107- Fair Use:

- ***Sega Enterprises, Ltd.* v. *Accolade, Inc.*(1992):**

"where **decompilation**is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a **legitimate reason** for seeking such access, decompilation is a fair use of the copyrighted work, as a matter of law."

***Sony Computer Entertainment, Inc.* v. *Connectix Corp.*, (2000)-**

- The *Sony* ruling undermined the "legitimate reason" requirement set forth in the *Sega* rule by reasoning that a final product which does not contain any code of the original product is transformative. A transformative product does not supplant the original product and thus does not cause a substantially adverse impact on the potential market of the original.
- Connectix virtual game station is modestly transformative. The product creates a new platform, the personal computers, on which consumer can play

games designed for the Sony play station. This innovation affords opportunities for game play in new environment specifically anywhere a Sony PlayStation console and television are not available, but a computer with a CD- ROM drive is more important the virtual game Station itself is a wholly new product notwithstanding the similarity of users and function between the Sony play station and the virtual game station.

- **Sec. 52 (1) (ab) Indian Copyright Act**
- (ab) doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer program with other programs by a lawful possessor of a computer program provided that such information is not otherwise readily available;
- Section 52(1):*"(aa) the making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme, from such copy-*

(i) in order to utilise the computer programme for the purposes for which it was supplied; or

(ii) to make back-up copies purely as a temporary protection against loss, destruction or damage in order only to utilise the computer programme for the purpose for which it was supplied;"

- *(ac)the observation, study or test of functioning of the computer program in order to determine the ideas and principles which underline any elements of the program while performing such acts necessary for the functions for which computer program was supplied;*
- *(ad)the making of copies or adaptation of the computer program from a personally legally obtained copy for non- commercial personal use;"*

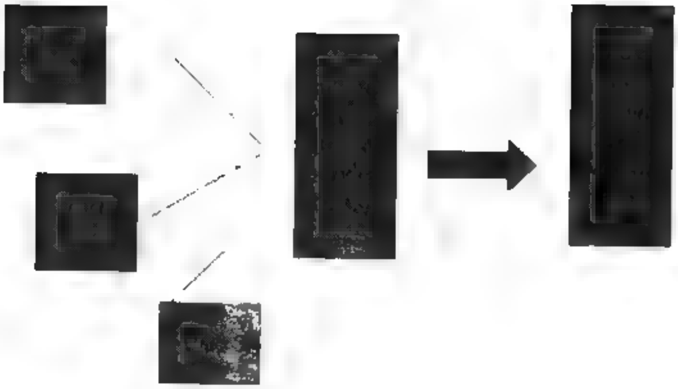
EU Software Directive: Art 6 (1)-Decompilation

- "1. The authorization of the right holder shall not be required where reproduction of the code and translation of its form within the meaning of article 4(a) and 4(b) are indispensable to obtain the **information necessary to achieve the interoperability** of an independently created computer program with other programs, provided that the following condition are met:

- These acts are performed by the **licensee or by another person having a right** to use a copy of a program, on their behalf by a person authorized to do so;
- The information necessary to achieve interoperability has **not previously been readily available** to the persons referred to in subparagraph(a); and
- These acts are confined to the **parts of the original program** which are necessary to achieve interoperability."

Copyright infringement in digital space:

- Direct infringement
- **Kelly v. Arriba Soft Corp. (2003).**
- Thumb nail image – image attribution page
- Created the thumb nail image using the software crawls and created the search engine by Arriba
- Whether thumb nail image is a copyright infringement of full size image of the Kelly photograph.
- Transformative test- Whether the new work merely supersedes the object of original creation or instead adds something new with a further purpose or different character, altering the first with new expression, meaning or message, it asks in other words whether and to what extent the new work is transformative.
- Although Arriba made exact replications of Kelly's images, the thumbnails were much smaller, lower resolution images that served an entirely different function than Kelly's original images. Kelly's images are artistic works intended to inform and to engage the viewer in an aesthetic experience. Arriba's search engine function as a tool to help index and to improve access to images on the internet and their related web sites.
- **Liability of internet service providers- Religious technology center v. Netcom on line Communication services inc (1995).**



- Ratio ….The court does not find workable a theory of infringement that would hold the entire internet liable for activities that cannot reasonably be deterred. Billions of BITS of data flow through the internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from non infringing bits. Because the court cannot see any meaningful distinction between the Netcom(without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement.

Safe Harbour Clause – Limiting the liability of internet service provider-

1. **Mere conduit**
2. **System catching**
3. **Search engine**
4. **Providing a platform to store information**

<u>Anti Circumvention Law:</u>

<u>WIPO Internet Treaties 1996:</u>

- Art 11 of WIPO Copyright Treaty 1996

"Contracting Parties shall provide **adequate legal protection** and **effective legal remedies** against the circumvention of **effective technological measures** that are used by authors in connection with the **exercise of their rights** under this treaty or the Berne Convention and that restrict acts, in respect of their **works,** which are not authorized by the authors concerned or permitted by law."

DMCA 1998.(Digital Millennium Copyright Act):

- Provisions granting a new form of legal protection to those who deploy **technological measures** to protect copyrighted works from unauthorized access, use or copying.

Sec 1201 (a) (1) (A):

- Forbids **circumvention** of effective **technical measures** used by copyright owners to protect access to their works.
- **technical measures means** "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Circumvention:

- Circumvention means to **"descramble a scrambled** work, to **decrypt an encrypted** work, or otherwise avoid, bypass, remove, deactivate, or impair a technological measure".

Individual Acts of Circumvention:

- **Access Protection Measures**: Prohibition : § 1201 (a) (1)
- **Right Protection Measures: Prohibition** : None

Manufacturing or Offering Devices that Circumvent:

- **Access Protection Measures**: Prohibition: § 1201 (a)(2)
- **Rights Protection Measures**: Prohibition : § 1201 (b)

Sec-1201 (f)- Reverse Engineering –

- Section 1201 (f) Reverse Engineering – (1) Notwithstanding the provisions of sub section (a)(1)(A). a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

- Section 1201 (f)(2) Notwithstanding the provision of subsection (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.
- Section 1201 (f)(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, pro-vides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.
- Section 1201 (f)(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.
- ***Universal City Studios, Inc.* v.*Reimerdes (2000) –***

  The reverse engineer could not raise the fair use defense as a defense against DMCA liability for unauthorized circumvention or trafficking in a circumvention device, even though the resulting use of the copyrighted program to be decompiled could be excused as a fair use.

EU Copyright Directive -Article 6 –Obligations as to technological measures:

1. Member states shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge or with reasonable grounds to know that he or she is pursuing that objective.

2. Article 6 (4) Notwithstanding the legal protection provided for in paragraph 1, in the absence of **voluntary measures** taken by right holders, including agreement between right holders and other parties concerned, Members states shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5 (2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b), or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject –matter concerned.

Section 65 A of the Copyright Amendment Act 2012 :

- (1) Any person who circumvents an **effective technological measure** applied for the purpose of protecting any of the **rights** conferred by this Act, with the **intention** of infringing such rights, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine.
- (2) Nothing in sub- section (1) shall prevent any person from, -

  (a) doing anything referred to therein for a purpose not expressly prohibited by this Act:

  Provided that any person facilitating circumvention by another person of a technological measures for such a purpose shall maintain a complete record of such other person including his name, address and all relevant particulars necessary to identify him and the purpose for which he has been facilitated.

Digital Distribution of Copyrighted Material

The digital distribution of copyrighted material such as music through the internet is another major form of copyright infringement. The primary mode of distribution is through peer-to-peer file sharing sites and online bulletin board services.

Peer-to-Peer File Sharing - the Napster case: Peer-to-peer file sharing, or P2P file sharing, allows users to access and share media files such as music, movies, books, games, etc. over the internet using P2P software. The P2P site enables the users to search for and locate the desired file on the computer of other users, which are interconnected through the P2P software. The file can then be directly downloaded from the other user's computer. Several copyright issues that arise through the P2P file sharing system were discussed in the Napster case in the US, including:

(i) Direct Copyright Infringement by the Users.

(ii) Use of the Fair Use Defence.

(iii) Contributory Copyright Infringement by the Intermediary,

(iv) Vicarious Copyright Infringement by the Intermediary.

(v) Applicability of Safe Harbor Provisions.

1. **The Napster Case** - Facts:The Napster case is the landmark decision given by the United States Court of Appeals in the Ninth Circuit with respect to peer-to-peer file sharing. In this case, Napster had designed and operated a P2P file sharing system which permitted the transmission and retention of sound recordings employing digital technology. The system facilitated the transmission of MP3 files, which were created through a process colloquially called "ripping", between and among its users. Napster's 'MusicShare' software, made the MP3 files available free of charge from Napster's Internet site. Through a process commonly called "peer-to-peer" file sharing, Napster allows its users to:

(i) make MP3 music files stored on individual computer hard drives available for copying by other Napster users;

(ii) search for MP3 music files stored on other users' computers; and

(iii) transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet.

The Napster site functioned as follows:

(i) Access: A user must first access Napster's Internet site and download and install the "MusicShare" software to his individual computer, after which the user can access the Napster system.

(ii) Listing of Files by the User: The user then creates a "user library" directory on his computer's hard drive, and saves his MP3 files in thelibrary directory. Once uploaded to the Napster servers, the user's MP3 file names are stored in a server-side "library".

(iii) Searching for Files: The files can be searched for by a user either through Napster's "search index" of its collective directory, or through its "hotlist function".

(iv) Transferring Files: To transfer a copy of the contents of a requested MP3 file, the Napster server software obtains the Internet address of the requesting user and the Internet address of the "host user" (the user with the available files). The requesting user's computer uses this information to establish a connection with the host user and downloads a copy of the contents of the MP3 file from one computer to the other over the Internet, "peer-to-peer."

The findings of the Court affirming the decision of the United States District Court for the Northern District of California, which found Napster liable for copyright infringement, are given below:

(a) Direct Infringement of Copyright: The first finding of the District Court that was upheld in appeal was that the users of the Napster site were engaged in the wholesale reproduction and distribution of copyrighted works, all constituting direct infringement. The requirements to be satisfied by the plaintiff's for proving direct infringement were as follows:

(i) they must show ownership of the allegedly infringed material, and

(ii) they must demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders.

The Court found that the plaintiffs had sufficiently demonstrated ownership of the material. It was also found that the Napster users violated at least two of the exclusive rights of a copyright holder- the Napster users who had uploaded file names to the search index for others to copy violated plaintiffs' distribution rights, while the Napster users who had downloaded files containing copyrighted music violated the plaintiffs' reproduction rights.

(b) Defence of Fair Use: Napster contended that its users were not directly infringing the plaintiff's copyrights because the users were engaged in fair use of the material. For the determination of whether the Napster users were engaged in fair use, firstly, the following factors, as listed in 17 U.S.C. § 107 were taken into consideration, and secondly, the fair uses alleged by Napster were considered.

Factors under 17 U.S.C. § 107:

(i) Purpose and Character of the Use: For determining the purpose and character of use, the Court considered the following:

(a) Was the use transformative: The Court considered whether the new work merely replaces the object of the original creation or instead adds a further purpose or different character .The Court observed that courts have generally been reluctant to find fair use when an original work is merely retransmitted in a different medium. The District Court's conclusion that downloading MP3 files does not transform the copyrighted work was upheld in appeal.

(b) Was the use commercial/ non-commercial: Direct economic benefit was not required to demonstrate a commercial use. Rather, repeated and exploitative copying of copyrighted works, even if the copies are not offered for sale, may constitute a commercial use . The Napster users were found to be engaged in commercial use of the copyrighted materials because "a host user sending a file cannot be said to engage in a personal use when distributing that file to an anonymous requester" and "Napster users get for free something they would ordinarily have to buy". Therefore, commercial use was also demonstrated by the repeated and exploitative unauthorised copies of copyrighted works.

(ii) Nature of the Copyrighted Work: Works that are creative in nature are "closer to the core of intended copyright protection" than are more fact-based works. The appellate Court upheld the District Court's determination that the plaintiffs' copyrighted musical compositions and sound recordings were creative in nature, and therefore went against a finding of fair use.

(iii) Amount and Substantiality of the Portion Used: The district court determined that Napster users engaged in "wholesale copying" of copyrighted work because the file transfer necessarily "involved copying the entirety of the copyrighted work". The Court upheld this, taking note that under certain circumstances, a court may conclude that a use is fair even when the protected work is copied in its entirety.

(iv) Effect of the Use upon the Potential Market for the Work: The proof required to demonstrate present or future market harm varies with the purpose and character of the use:

"A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work If the intended use is for commercial gain, that likelihood [of market harm] may be presumed. But if it is for a noncommercial purpose, the likelihood must be demonstrated."

The Court upheld the District Court's finding that Napster harmed the market for the plaintiffs in at least two ways- it reduces audio CD sales among college students, and it "raises barriers to plaintiffs' entry into the market for the digital downloading of music, since having digital downloads available for free on the Napster system necessarily harmed the copyright holders' attempts to charge for the same downloads.

2. Fair Uses Alleged by Napster: The following fair uses were alleged by Napster:

(i) Sampling: Napster contended that its users downloaded the MP3 files to "sample" the music in order to decide whether to purchase the recording. It was held that sampling remains a commercial use even if some users eventually purchase the music. The Court also took into consideration that the plaintiff collected royalties for their 36 second long song samples available on retail Internet sites, which were self-programmed to time out. In comparison, Napster users could download a full, free and permanent copy of the recording.

(ii) Space-shifting: Napster alleged that space shifting of musical compositions and sound recordings was previously held to be a fair use. Space-shifting occurs when a Napster user downloads MP3 music files in order to listen to music he already owns on audio CD. The Court, however, refused to apply the decisions on space shifting to the Napster case, since the time or space-shifting discussed in the previous judgments did not also simultaneously involve distribution of the copyrighted material to the general public; it exposed the copyrighted material only to the original user.

The Appellate Court therefore upheld the District Court's determination that the Napster users do not have a fair use defense.

3. Contributory and Vicarious Copyright Infringement: Napster was found to be secondarily liable for the direct infringement under two doctrines of copyright law: contributory copyright infringement and vicarious copyright infringement.

(i) Contributory Copyright Infringement: Contributory copyright infringement requires proof of:

(a) Knowledge: Traditionally, one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer.

The Court discussed the concept of contributory infringement as discussed in the Sony case, where the Court refused to hold the manufacturer and retailers of video tape recorders liable for contributory infringement despite evidence that such machines could be and were used to infringe the plaintiffs' copyrighted television shows. Sony stated that if liability "is to be imposed on petitioners in this case, it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make unauthorized copies of copyrighted material." The Sony Court declined to impute the requisite level of knowledge where the defendants made and sold equipment capable of both infringing and "substantial non-infringing uses".

The Appellate Court, though refusing to impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights, nevertheless found that Napster had sufficient knowledge, both actual and constructive, of direct infringement. The Court upheld the District Court's finding that Napster, by its conduct, knowingly encouraged and assisted the infringement of plaintiffs' copyrights.

(b) Material Contribution: A secondary infringer is required to "know or have reason to know" of direct infringement. The Court also found that Napster materially contributed to the infringing activity. It was concluded that "without the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts."

Thus, the Court found that Napster had knowledge of and had materially contributed to the infringement, and was, therefore, liable under the doctrine of contributory copyright infringement.

(ii) Vicarious Copyright Infringement: In the context of copyright law, vicarious liability extends beyond an employer/employee relationship to cases in which a defendant "has the right and ability

to supervise the infringing activity and also has a direct financial interest in such activities."

(a) Financial benefit: The District Court determined that plaintiffs had demonstrated they would likely succeed in establishing that Napster has a direct financial interest in the infringing activity. The Appellate Court agreed with this, observing that financial benefit existed where the availability of infringing material "acts as a 'draw' for customers." Ample evidence supported the district court's finding that Napster's future revenue was directly dependent upon increases in its user base.

(b) Supervision: The plaintiffs demonstrated that Napster retained the right to control access to its system, through a "reservation of rights policy", on its website that it expressly reserves the "right to refuse service and terminate accounts in [its] discretion, including, but not limited to, if Napster believes that user conduct violates applicable law ... or for any reason in Napster's sole discretion, with or without cause."

The Court held that the District Court had correctly determined that Napster had the right and ability to police its system, and failed to exercise that right to prevent the exchange of copyrighted material.

Thus, the Court found that Napster had financially benefited from the infringement and had failed to exercise its powers of supervision, and was, therefore, liable under the doctrine of vicarious copyright infringement.

4. Safe Harbor Provisions under Copyright Law: The District Court recognized that a preliminary injunction against Napster's participation in copyright infringement was not only warranted but required. Napster asserted protection under the safe harbor rules of the Audio Home Recording Act and the Digital Millennium Copyright Act as defences for the injunction that was granted against it.

5. [US] Audio Home Recording Act: The relevant provision of this Act is:

"No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the non-commercial use by aconsumer of such a device or medium for making digital musical recordings or analog musical recordings."

Napster contended that the MP3 file exchange is the type of "non-commercial use" as protected from infringement actions by the statute. This argument was rejected on the ground that the Audio Home Recording Act is "irrelevant" to the action because the Audio Home Recording Act does not cover the downloading of MP3 files to computer hard drives.

6. [US] Digital Millennium Copyright Act: Napster also argued based on the statutory limitation on liability by asserting the protections of the "safe harbor" from copyright infringement suits for "Internet service providers" contained in the Digital Millennium Copyright Act. The District Court did not give this statutory limitation any weight favoring a denial of temporary injunctive relief. The court concluded that Napster "has failed to persuade this court that subsection 512(d) shelters contributory infringers."

On appeal, the Court did not accept a blanket conclusion that § 512 of the Digital Millennium Copyright Act will never protect secondary infringers. The Court instead recognized the following issues to be fully developed at trial:

(i) Whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d);

(ii) Whether copyright owners must give a service provider "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and

(iii) Whether Napster complies with § 512(i), which requires a service provider to timely establish a detailed copyright compliance policy.

Bulletin Board Systems

Bulletin board systems are similar to P2P File sharing systems, where the software allows users to connect and log into a computer system using a terminal program. The users can upload and download software, data, share news, e-mail or chat with other users and even play online games.

In the case of Playboy Enterprises, Inc v George Frena, the defendant opened a subscription BBS, where photographs copyrighted by the plaintiff were uploaded for without the required permission. The BBS was accessible for a fee via telephone modem to customers. Once logged in, the users could browse through the pictures as well as download them onto their home computers. The U.S. District Court for the Middle District of Florida held that the defendant had violated the plaintiffs exclusive right to distribute and display its copyrighted works. The defendant's argument that the images had not been uploaded by him, but were uploaded by the subscribers to his system, was rejected. The Court

found that neither knowledge nor intention was an essential ingredient of infringement under the U.S. Copyright Act, and the defendant had supplied a product which contained unauthorized material. The Court further rejected the fair use of defence on the grounds that:

(i) The use of the work was commercial.

(ii) The nature of the copyrighted works was in the category of fantasy and entertainment.

(iii) A substantial amount of the plaintiff's copyrighted work is used, since the pictures are a major factor for the success of its magazine.

(iv) The effect of the use on the potential market of the plaintiff's work was found to be adverse if the conduct of the defendant were to become very widespread.

On these grounds, the defendant was found to be liable for copyright infringement

Patenting of Software

Article 27.1 of the TRIPS Agreement as discussed above, indicates that software may also be patented subject to the fulfillment of the three criteria mentioned, i.e., it must be new, it must involve an inventive step and must be capable of industrial application. The main drawback of copyright is that it protects only the expression of the software, the protection does not extend to the underlying ideas, which are often of immense commercial value. Despite this, there are still many advantages that a copyright offers. Patents, as opposed to copyright, need to fulfill more stringent technical and scientific criteria in order to qualify for protection, which vary from one country to another. As a result, patents need to be filed in every country in which protection is sought, while international protection of copyright is automatic. Finally, the period of protection for a patent is shorter, usually for about 20 years, while copyright protection is usually of 50 years or more.

1. Patenting of Computer Programmes under Indian Patent Act: The Indian Patent Act specifically excludes 'computer programmes per se' from the scope of the term 'inventions'.

An amendment made to section 3(k) of the Indian Patents Act, 1970, through the Patents (Amendment) Ordinance, 2004 was later rejected, and was not included under the Patents (Amendment) Act of 2005. The amended clause was to read as follows:

"(k) a computer programme per se other than its technical application to industry or a combination with hardware ".

It is therefore unclear, if, patents may be granted for computer programmes which have technical application to industry or for computer programmes that work in combination with hardware.

Software is a patentable subject matter-

- Art 27 TRIPS Agreement "patent shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are **new**, involve an **inventive step** and are **capable of industrial application**…., patent shall be available and patent rights enjoyable without discrimination as to the place of invention, the field of technology and whether product are imported or locally produced."
- Sec 3 (k) of the Patent Act 1970

"A mathematical or business method or a **computer program per se or algorithm**" is not patentable.

35 USC § 101:

- "Whoever invents or discovers any new and useful **process, machine, manufacture,** or **composition of matter,** or any new and useful improvement thereof, may obtain a patent thereof, subject to the conditions and requirements of this title."
- Laws of nature, abstract ideas and mathematical formula are also not patentable.

Gottschalk v. Benson (1972):

- Claim – a method for programming any type of general purpose digital computer to convert binary coded decimal numerals into pure binary numerals, such claim is not being limited to any particular art or technology to any particular apparatus or machinery or to any particular end use.

- Whether the method described and claimed is a "process" within the meaning of the Patent Act.

Ratio:

- It was held that the conversion method involved in the instant proceedings was not a "process" within the meaning of the pertinent provisions of the Patent Act and thus could not be patented since,

(1) The method was so abstract as to cover both known and unknown uses of the binary- coded- decimal to pure binary conversion,

(2) The end use could vary and could be performed through any existing machinery or future devised machinery or without any apparatus,

(3) The mathematical formula involved had no substantial practical application except in connection with a digital computer,

(4) The result of granting a patent would be to improperly issue a patent for idea (algorithm)

- Mental Step Doctrine
- Pre empt the mathematical formula.

<u>Parker v. Flook (1978):</u>

- A patent on a method for updating alarm limits during catalytic conversion processes.
- Whether the identification of a limited category of useful, though conventional, post solution applications of such a formula makes respondents method eligible for patent protection?
- During the catalytic conversion processes operating conditions such as temperature, pressure and flow rates are constantly monitored.

The method consists of three steps:

(1) An initial step which merely measures the present value of the process variable

(2) An intermediate step which uses an algorithm to calculate an updated alarm-limit value

(3) A final step in which the actual alarm limit is adjusted to the updated value.

The only difference between the conventional methods of changing alarm limits and that described in respondent's application rests in the second step- the mathematical algorithm or formula.

Ratio:

- The method for updating alarm limits was not patentable under § 101 of the Patent Act, the identification of a limited category of useful though conventional, post –solution applications of the formula not making the method eligible for patent protection.
- Post solution activity

  The notion that post –solution activity, no matter how conventional or obvious in it, can transform an unpatentable principle into a patentable process **exalts form over substances.** A competent draftsman could attach some form of post –solution activity to almost any mathematical formula, the Pythagorean theorem would not have been patentable or partially patentable because a patent application contained a final step indicating that the formula when solved could be usefully applied to existing surveying techniques.

Diamond v. diehr (1981):

- Process for molding raw, uncured synthetic rubber into cured precision products. The individuals claimed that their process insured the production of molded articles which are properly cured. Although it is possible by using well-known time, temperature and cure relationships to calculate by means of an established mathematical equation when to open the molding press and remove the cured product, the individuals argued that the industry had not been able to obtain uniformly accurate cures because the temperature of the press could not be precisely measured, making it difficult to do the necessary computation to determine cure time.

Ratio:

- When a claim containing a mathematical formula implements or applies the formula in a structure or process which when considered as a whole is performing a function which the patent laws were designed to protect (e.g., **transforming or reducing an article to a different state or thing**) then the claim satisfies Sec 101 requirements.

- The physical and chemical process for molding precision synthetic rubber products fell within the categories of subject matter eligible for patent protection and this result was not altered by the fact that in several steps of the process a mathematical equation and programmed digital computer were used, since

  1. No attempt was being made to pre empt the use of the equation(Arrhenius equation) but only to foreclose others from the use of that equation in conjunction with all of the other steps in the claimed process, and
  2. Use of the computer in the process did not render the process as a whole unpatentable subject matter in view of the fact that the computer was used to achieve a result previously unknown in the art, the fact that one or more of the steps in the process might not, in isolation, be novel or independently eligible for patent protection being irrelevant to the question of whether the claims as a whole recited subject matter eligible for patent protection.

Freeman-Walter-abele test:

- This test consists of two steps:

(1) The claim is analyzed to determine whether a mathematical algorithm is directly or indirectly recited; and

(2) if a mathematical algorithm is found, the claim as a whole is further analyzed to determine whether the algorithm is applied in any manner to physical elements or process steps

If the answer to the second question is "yes" the claimed invention is patentable subject matter.

Freeman:

- The subject matter of Freeman's invention is a system for typesetting alphanumeric information, using a computer based control system in conjunction with a phototypesetter of conventional design.

Walter:

- In Walter, the claims were directed to a process for correlating and cross – correlating signals. All of the claims steps were algorithm steps for performing the correlation or cross- correlation. There were no limitations in the claims, other than a field of use set forth in the preamble of the claims which stated that the algorithm was for use in connection with **seismic surveying.**

Abele:

- Invention is in the field of image processing particularly as applied to computerized axial tomography or CAT Scans. Specifically, an appellant invention is directed to improvement in computed tomography whereby exposure to x-ray was reduced while reliability of produced image is improved.

<u>In re kuriappan P. Alappat:</u>

- Alappat's invention relates generally to a means for **creating a smooth waveform display in a digital oscilloscope**. The screen of an oscilloscope is the front of a cathode-ray tube (CRT), which is like a TV picture tube, whose screen, when in operation, presents an array (or raster) of pixels arranged at intersections of vertical columns and horizontal rows, a pixel being a spot on the screen which may be illuminated by directing an electron beam to that spot, as in TV. Each column in the array represents a different time period and each row represents a different magnitude.

- An input signal to the oscilloscope is sampled and digitized to provide a waveform data sequence (vector list), wherein each successive elements of the sequence represents the magnitude of the waveform at a successively later time. The waveform data sequence is then processed to provide a bit map, which is a stored data array indicating which pixels are to be illuminated. The waveform ultimately displayed is formed by a group of vectors, wherein each vector has a straight line trajectory between two points on the screen at elevations representing the magnitudes of two successive input signal samples and at horizontal positions representing the timing of the two samples.

<u>Arrhythmia research technology inc. v. corazonix corporation (1992):</u>

- The invention claimed is directed to the analysis of electrocardiographic signals in order to determine certain characteristics of the heart function. In the hours immediately after a heart attack (myocardial infraction) the victim is particularly vulnerable to an acute type of heart arrhythmia known as ventricular tachycardia. Ventricular tachycardia leads quickly to ventricular fibrillation, in which the heart ceases effectively to pump blood through the body.

◉ An input signal to the oscilloscope is sampled and digitized to provide a waveform data sequence (vector list), wherein each successive elements of the sequence represents the magnitude of the waveform at a successively later time. The waveform data sequence is then processed to provide a bit map, which is a stored data array indicating which pixels are to be illuminated. The waveform ultimately displayed is formed by a group of vectors, wherein each vector has a straight line trajectory between two points on the screen at elevations representing the magnitudes of two successive input signal samples and at horizontal positions representing the timing of the two samples.

State street bank & trust Co. v. Signature Financial Group, inc. (1998) Business Method:

◉ The invention is directed to a data processing system for implementing an investment structure which was developed for use in Signature's business as an administrator and accounting agent for mutual funds. In essence, the system, identified by the proprietary name Hub and Spoke, facilitates a structure whereby mutual funds pool their assets in an investment portfolio organized as a partnership. This investment configuration provides the administrator of a mutual fund with the advantageous combination of economies of scale in administering investments coupled with the tax advantages of a partnership.

◉ **Ratio…**

◉ Law of nature, natural phenomena, and abstract ideas can never be the subject of patents.

◉ Practical applications provide **"useful, concrete and tangible results".**

Bilski v. kappos (2010) business method:

- **"Energy risk Management Method"**

  Their invention relates to a method practiced by a commodity provider, such as the provider of the energy. The method enables the provider to manage (or "hedge") the consumption risks associated with a commodity sold at a fixed price. Energy consumers face two kinds of risk: price risk and consumption risk. For the energy supplier, price risk is relatively easy to manage. Simply establish the fixed price based on historical averages. Managing consumption risk is more difficult. Energy consumption will fluctuate in an unpredictable way, owing to changes in the weather.

- Kennedy J.

  The machine -or-transformation test may well provide a sufficient basis for evaluating processes similar to those in the industrial age- for example, inventions grounded in a physical or other tangible form. But there are reasons to doubt whether the test should be the sole criterion for determining the patentability of inventions in the information age.

Alice Corporation Pty. Ltd. v. C.L.S. Bank International

This is a landmark judgment given in 2014 by the US Supreme Court on the patentability of software. This judgment confirmed previous judgments that computer programs that amounted to an abstract idea, and if the claim as a whole did not amount to anything significantly more than the abstract idea in itself, then the program was not eligible for patent protection. This judgment reinforced the ongoing global debate on the patentability of software.

The patents at issue, which belonged to the Appellant, disclosed a scheme for mitigating 'settlement risk', i.e., the risk that only one party to a financial exchange will satisfy its obligation, using a computer system as a third party intermediary. This scheme was styled as a method for exchanging financial obligations, a computer system configured to carry out the method and a computer-readable medium containing program code for causing a computer to perform the method.

The Respondents filed a suit against the Appellant seeking a declaratory judgment that the claims at issue were invalid, unenforceable or not infringed, while the Appellants filed a counter-suit alleging infringement of its patents by the

Respondents. The District Court held that these claims were ineligible because they were directed to the abstract idea of 'employing a neutral intermediary to facilitate simultaneous exchange of obligations in order to minimize risk'. A divided panel of the US Court of Appeals for the Federal Circuit reversed this decision on the grounds that it was not 'manifestly evident' that the claims were directed to an 'abstract idea'. The Respondents then petitioned the same Federal Circuit Court for an en banc hearing. This resulted in a fractured panel of seven different opinions by ten judges. A majority of 5 judges reversed the decision and held that the claims were patent ineligible, without addressing the issues relating to patentability of software. As a result, the Appellant applied for a writ of certiorari with the US Supreme Court.

The Supreme Court found that the appellant's first claim to the method was ineligible because it amounted to an abstract idea, which was ineligible for a patent as per the test of Mayo Collaborative Services v. Prometheus Laboratories, Inc..The claim was found to be 'nothing significantly more' than an instruction to apply the abstract idea of intermediated settlement, which was a fundamental economic practice long prevalent in the system of commerce, using some unspecified, generic computer. The second and third claims were also found to be ineligible for the reason that the combination with computers did not transform the abstract idea into a patent-eligible invention, as per the rule laid down in Bilski v. Kappos. It was found that the generally-recited computers in the claim were merely linked to the method for use, and added nothing of substance to the underlying abstract idea.

Notably, the judgment did not specifically exclude computer programs from patentability, nor did it impose any special requirements for eligibility of software and business models. The Court emphasized the difference between patents that claim the 'building blocks' of human ingenuity, and those that integrate the building blocks into something more, finding that only the latter were patent - eligible. Examples of abstract ideas that were considered in the judgment as patent-ineligible include:

(i) Fundamental economic practices;

(ii) Certain methods of organising human activities;

(iii) An idea in itself;

(iv) Mathematical relationships or formulas

The following were listed as examples of claims that contained an abstract idea, but, as a whole amounted to significantly more than the abstract idea itself:

(i) Improvements to another technology or technical field.

(ii) Improvements to the functioning of the computer itself.

(iii) Meaningful uses beyond generally linking the use of an abstract idea to a particular technological environment.

The following were listed as examples of claims that contained an abstract idea, but, as a whole did not amount to significantly more than the abstract idea itself:

(i) Mere instructions to implement an abstract idea on a computer.

(ii) Requiring no more than a generic computer to perform generic computer functions that were well-understood, routine and conventional activities previously known to the industry.

Preliminary Examination Instructions: The US Patent and Trademark Office issued the following Preliminary Examination Instructions to be applied for the determination of subject matter eligibility for patents on the basis of this judgment:

(i) First determine whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does not fall into one of the categories; reject the claim as being directed to non-statutory subject-matter.

(ii) Next, if the claim falls within one of the statutory categories, determine whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon and abstract idea) and if so, determine whether the claim is a patent-eligible application of an exception.

ONLINE TRADEMARK INFRINGEMENT

Traditional forms of trademark infringement, such as passing off, use of a deceptively similar mark, copying a mark, etc., find a new medium for commission in cyberspace. In addition to this, new forms of infringement unique to cyberspace have been created, such as cybersquatting, reverse domain name hijacking, use of a trademark in a metatag, keyword infringement, etc.

Law on Trademarks in India

Law on Trademarks in India: Indian law protects trademark under the provisions laid down in Trademarks Act, 1999 (the Trademarks Act). The Act was enacted to comply with the provisions of the Paris Convention and the TRIPS Agreement, Article 15- 21 of which contain the provisions related to the protection of trademarks. The Trademarks Act was amended in 2010 to comply with the Madrid Protocol.

Summary of Important Provisions of Trademark Act, 1999: Section 2 (zb) of Trademark Act, 1999 defines a "trademark" as a mark which is capable of being represented graphically and which can distinguish the goods and services of one person from those of others. It may include shape, color combination and packaging of goods.

Section 28 of the Act gives exclusive rights of the use of trademark to the registered proprietor of the trademark. The term of a trademark is for a period of ten years which may be renewed from time to time in accordance with the provisions of Section 25. Section 18-26 lays down the procedure for registration of a trademark, which may be renewed from time to time. While registration of a trademark is not obligatory, Section 27 prevents the holder of an unregistered trademark from bringing an action for infringement if his mark is utilized by others.

A trademark is infringed as per the provisions of Section 29 of Trademark Act, 1999 if a person not being a proprietor of registered trademark or a person, other than the person permitted to use the trademark, uses a mark that is identical with or deceptively similar to the registered trademark. There are several exceptions to this section given under Section 30 of the Act which provides that there will not be an infringement of trademark if the use of trademark is it is used in accordance with honest practices in industrial and commercial matters and no unfair advantage or disrepute is being caused to the trademark.

Section 134 of the Act lays down the jurisdiction of courts in cases related with infringement of trademark and no court inferior to District Court can initiate the suit regarding infringement of trademark. The remedies in a suit of infringement can range from an injunction to damages which can be granted by the Court under Section 135.

International Trademarks

Chapter IV A inserted by way of amendment through the Trademark Amendment Bill, 2010 lays special provisions related to the protection of trademarks through international registration under the Madrid protocol. India is a signatory to Madrid Protocol which is a simple and effective system of registering international trademarks. Compliance with the Madrid Protocol through Chapter IVA now permits a one-time registration through a single form and a one-time payment of fees for a trademark that will have validity in all the signatories of the Protocol.

Domain Name Disputes

What are Domain Names: A domain name is the human friendly name of an Internet address. It is technically known as a "Unique Resource Locator", or URL. The actual name of a website is in the form of an "Internet Protocol address", or IP address. For example, one IP address of Google is 216.239.51.104. Such sets of number can be quite difficult to remember, unlike the URL of Google, which is "www.google.com". Thus a domain name is a unique alias for an IP address, and the system that locates and translates a domain name into an IP address and vice versa is known as a domain name system. A domain name system exists in the form of databases around the world, and is commonly referred to as the address book of the internet.

1. The ICANN: It is essential that domain names be unique across the globe, in order to enable one computer to find another. The ICANN, or the Internet Corporation for Assigned Names and Numbers, is the body responsible for the coordination of domain names around the world. It is an internationally organized non-profit corporation, with membership from different countries and experts in the field. The ICANN is the coordinator of the functions of the IANA,

or the Internet Assigned Numbers Authority, which is responsible for managing the DNS root zone, i.e., the gTLDs and the ccTLDs, along with the allocation of internet numbering resources.

2. Domain Levels:

(i) Top Level Domains

At the top of the domain name hierarchy are top level domains, or TLDs, which are of two types- generic TLDsorgTLD, and country-code TLDs, or ccTLDs.. Examples of gTLDs are .com', '.biz', '.info', etc. For a country, the top level domain is the country code top level domain, or the ccTLD. The label for a ccTLD consists of two character abbreviations of the name of the country, for example, India's ccTLD is '.in', the ccTLD for the US id '.us', etc. There are currently 252 ccTLDs reflected in the database of the Internet Assigned Numbers Authority (IANA). This numberissubject to change based on the creation of new countries.

(ii) **Second Level Domains**

Every domain name ends with the label of a TLD. Ina domain name, the label that precedes the TLD constitutes the second level domain. For example, in 'www.google.com', '.com' constitutes the TLD, while 'Google' constitutes the second level domain.

Registration of Domain Names: The registration of domain names can be discussed under the following heads:

(a) Registration of ccTLDs: The administration of ccTLDs lies with the ICANN. In order to acquire a particular domain name, they have to be registered at a domain name registrar. Until 1999, registration of .com, .net and .org domains was handled by Network Solutions Inc., or NSI. Post 1998, following an anti-trust suit againstNSI in 1997, this was replaced with a system of multiple registrars under the supervision of the ICANN. These domain name registrars are required to be accredited by the ICANN. For example, BigRock Solutions Ltd., Good Domain Registry Pvt. Ltd.,etc. are some Indian domain name registrars which are accredited by the ICANRT .

(b) Registration of ccTLDs: The administration of ccTLDs, on the other hand, lies with each respective country, and is to be done in accordance with the guidelines of the ICANN. The INF.egistry is India's official '.in' domain name registry, and is operated under the authority of NIXI, the National Internet Exchange of India. Within India, the National Informatics Centre, NIC, is the exclusive Government registrar for 'gov.in' and 'mil.in' domains, while ERNET is the exclusive registrar for 'ac.in', 'edu.in' and 'res.in'. These government registrars, along with several other registrars have been accredited by the INRegistry. Some general registration policies of this registry are:

(i) Registration may be for a minimum period of 1 year and a maximum period of 10 years.

(ii) The domain names are between 3 and 63 characters in length, consisting of letters, digits and hyphens only.

(iii) Single and double character domain names are reserved by the government and NIXI, and are not available to the public.

(iv) The following category of names are reserved- constitutional authorities, names of states, union territories and cities, and certain other specific names for use by the Registry.

(v) The zones of '.gov.in', '.mil.in', 'ac.in' and 'edu.in' are reserved for government, defence and educational institutions respectively.

(vi) Unlimited generic .in registration will be open to the public at the 2nd level and the 3rd level in popular zones like '.co.in', '.net.in', etc.

(vii) Registrants are allowed to transfer domain names to the registrar of their choice.

The policy of domain name registration has been made extremely liberal and market friendly in a number of countries, in order to encourage a large number of registrations. This is because the number of registrations is seen as a measure of a country's popularity in the internet space, and as a means to facilitate the proliferation of internet in a country.

Types of Domain Name Disputes:

1. **Cybersquatting:** the registration of a domain name that consists of a mark that is identical to or confusingly similar to an existing trademark. Cybersquatting is constituted only if the registration has been done in **bad faith,** that is, with the intention of selling the domain name at a much higher price to the owner of the trademark, or diverting the consumers of the owner of the trademark, or to create an impression of having some kind of affiliation with the owner of the trade mark.

2. **Typo squatting:**It is a form of cybersquatting where the domain name that is registered incorporate a slight change in the spelling of a well-known trademark or domain name, usually in the form of a common typographical error made by internet users.

3. **Reverse domain name hijacking:** reverse domain name hijacking or reverse cybersquatting is an attempt by a trademark holder to acquire a domain name from a legitimate user by making false cybersquatting allegations against him.

Dispute Resolution in the UK: Trademarks Act 1994:

- Section 10 of this Act provides that the following constitute infringement of a trademark:
- Use of a sign identical to a registered trademark.
- Use of a sign identical or similar to a registered trademark for identical or similar goods and services which will create a likelihood of confusion.
- Use of a sign identical or similar to a registered trademark for goods and services that are not similar where the use takes unfair advantage of or is detrimental to the distinctive character or reputation of the registered trademark.
- Use of a sign in the form of affixation onto goods or packaging, offer for sale, import or export or in advertising.
- Use of a registered trademark on material intended for labeling or packing.
- Legitimate use of a mark which takes unfair advantage of or is detrimental to the distinctive character or reputation of the registered trademark.

Passing Off:

- Lord Diplock in ***ErvenWarnink v. J. Townend& Sons Ltd. (1979).***
- Essential Elements for passing off action as:

(1) Misrepresentation

(2) Made by a trader in the course of trade

(3) To prospective customers of his or ultimate consumer of goods or services supplied by him

(4) Which is calculated to injure the business or goodwill of another trader

(5) Which causes actual damage to a business or goodwill of the trader by whom action is brought or will probably do so?

Domain Name and Passing Off:

- **British Telecommunications PLC v. One In a million:**

Respondent had registered several domain names including British Telecommunication, Marks & Spencer, Sainsbury's, Virgin, and Ladbroke Group, and had written to these companies offering them for sale.

The court held that the domain names had been registered with the intention of taking advantage of the distinctive character and reputation of the trademark, which was unfair and detrimental.

- ... It follows that the registration by the appellants of the domain name including the name Marks & Spencer makes a false representation that they are associated or connected with Marks & Spencer PLC. This can be demonstrated by considering the reaction of a person who taps into his computer the domain name marksandspencer.co.uk and presses a button to execute a 'whois' search. He will be told that the registrant is One In A Million Limited. A substantial number of persons will conclude that One In A Million Limited must be connected or associated with Marks & Spencer PLC. That amounts to a false representation which constitutes passing off.

Dispute Resolution under the Indian Trademarks Act:

- Indian Courts in several matters granted protection to domain names under Trademark Law.
- **Trademark Act applied to passing off of domain names: Yahoo! Inc. v. AkashArora&Anr,** (1999) the case involved an action of passing off, where the defendant's domain name 'yahoo.india' provided services similar to the plaintiffs, and imitated their website in content, colour and scheme. While referring to several international case laws on the subject, the Delhi High Court extended the application of the Indian Trademark Act to domain names:
- **Passing off applies to service:** the law of trademark was applicable to services, including the services provided by a website.
- **Domain Name confusingly Similar:**yahoo!&yahooindia – the two marks are almost similar except for use of the suffix 'India' in the latter.
- Disclaimer cannot remedy appropriation of a trademark

Domain name –A Valuable Corporate Asset:

- **Rediff Communication Ltd v. Cyberbooth and Anr** (2000) an injunction was granted against the defendant for the use of the term 'Radiff' and the domain name 'radiff.com', on the grounds of likelihood of confusion and the apparent intention of the defendants to trade on the plaintiff's reputation. During the decision, the court observed the following with regard to the importance of protecting domain name as a trademark:

  The court observed the following with regard to the importance of protecting domain name as a trademark:

"what emerges from these authorities is that the Internet domain names are of importance and can be a **valuable corporate asset.** A domain name is more than an Internet Addresses and is entitled to the equal protection as trade mark. With the advancement and progress in the technology, the services rendered in the internet site have also come to be recognized and accepted and are being given protection so as to protect such provider of service from passing off the services rendered by others as his services. "

US: FEDERAL TRADEMARK DILUTION ACT:

- *Panavision International, LP v. Toeppen (1998):*
- Panavision holds registered trademarks to the names "panavision" & "panaflex" in connection with motion picture camera equipment. In 1995, Panavision attempted to register a web site on the internet with the domain name Panavision.com. It could not do that because Toeppen had already established a website using Panavision's trademark as his domain name. Toeppen's web page for this site displayed photographs of the City of Pana, illinois.
- Later Toeppen registered the other TM as the Domain Name Panaflex: displayed the word 'Hello'.
- Panavision alleged claims for dilution of its trademark under the Federal Trademark Dilution Act, 15 U.S.C. § 1125 (c). The section provides:

'the owner of a famous mark shall be entitled to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark…'

Issues:

A plaintiff must show that

(1) The mark is famous

(2) The defendant is making a commercial use of the mark in commerce

(3) The defendant's use began after the mark become famous, and

(4) The defendant's use of the mark dilutes the quality of the mark by diminishing the capacity of the mark to identify and distinguish goods and services.

COMMERCIAL USE:

- Toeppen's "business" is to register trademarks as a domain name and then sell them to the rightful trademark owners. Toeppen traded on the value of Panavision's marks. So long as he held the Internet registrations, he curtailed Panavision's exploitation of the value of its trademarks in the internet, a value which Toeppen then used when he attempted to sell the Panaavision.com domain name to Panavision.

DILUTION:

- Dilution is defined as the lessening the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception.
- The court found that Toeppen's conduct diminished "the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet."

ANTICYBERSQUATTING CONSUMER PROTECTION ACT 1999:

- The Anti-cyber-squatting Consumer Protection Act makes it illegal to register or use a domain name that corresponds to a trademark where the domain name registrant has **no legitimate interest** in using the name and acts in badfaith to deprive the trademark owner of the use of the name.
- **Section 125 (d) (1) (A) of the Act -**

A person shall be liable in a civil action by the owner of a mark… if, without regard to the goods or services of the parties, that person

(i) Has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) Registers, traffics in, or uses a domain name that-

(1) In the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark

(2) In the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark.

<u>Shields v. Zuccarini (2001):</u>

- Shield a graphic artist from Alto, Michigan,

creates, exhibits and markets cartoons under the names **"Joe cartoon" and "The Joe Cartoon Co."**

- On 1997, Shield registered the domain name joecartoon.com, and he has operated it as a web site ever since.
- Over 700,000 visits per month.
- In 1999 Zuccarini, registered five world wide web variations on Shields's site: **joescartoon.com, joecarton.com, joescartons.com, joescartoons.com and cartoonjoe.com.**
- Zuccarini's sites featured advertisements for other sites and for credit card companies.
- Shields was required to prove that

(1) "Joe Cartoon" is a distinctive or famous mark entitled to protection,

(2) Zuccarini's domain names are "identical or confusingly similar to" Shields's mark,

(3) Zuccarini registered the domain names with the bad faith intent to profit from them.

Use in Bad Faith-

- The following factors may be taken into consideration while determining if the person had a bad faith to profit from the mark:

(i) The person's trademark or IPR in that domain name, if any.

(ii) Extent of the person's legal name or identifier used in the domain name

(iii) Prior use in bona fide offering of goods or services

(iv) Bona fide non-commercial or fair use of the mark in the site.

(v) intention to divert consumers from the trademark owner's site.

(vi) Offer to sell, transfer, otherwise assign to the mark owner or a third party for financial gain.

(vii) provision of material and misleading false contact information while registering the domain name.

(viii) registration of identical or confusingly similar domain names to the marks of others.

(ix) extent to which the incorporated mark ıs not distinctive or famous.

Ratio:

- Zuccarini's conduct satisfies a number of these factors. Zuccarini has never used the infringing domain names as trademarks or service marks, thus he has no intellectual property rights in these domain names. He has never used the infringing domain names in connection with the bona fide offering of goods or services. He deliberately maintain these domain names to divert consumer from shields web site. In doing so, he harms the goodwill associated with the mark. He does this either for commercial gain, or with the intent to tarnish or disparage Shields mark by creating a likelihood of confusion.

ICANN Uniform Domain Name Dispute Resolution Policy 1999:

- Mandatory administrative proceeding
- The third party files a complaint that:
- 1. your domain name is identical or confusingly similar to a trademark or service mark in which the complaint has rights;
- 2. you have no rights or legitimate interest in respect of the domain name;and
- 3. Your domain name has been registered and is being used in bad faith.

Use in Bad Faith:

- Use of bad faith includes the following factors:

  (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out of pocket costs directly related to the domain name; or

  (ii) You have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

  (iii) You have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

  (iv) By using the domain name you have intentionally attempted to attract, for commercial gain, internet users to your web site or other on –line location, by creating a likelihood of confusion with the complaint's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your website or location.

Remedies:

- ***Cancellation***of your domain name or the ***transfer***of your domain name registration to the complainant.

Metatagging:

- Metatags are HTML code intended to describe the contents of the web site. There are different types of metatags:

  1. Description metatags: Description metatags are intended to describe the web site.
  2. Keyword metatags: Keyword metatags contain keywords relating to the contents of the web site.

Brookfield Communications, Inc. v. west Coast Entertainment Corporation.(1999):

- Brookfield Communication Inc. (TM) **"MovieBuff"** Brookfield gathers and sells information about the entertainment industry.
- West Coast :**"Movie Buff"** Service mark.

"The Movie Buff's Movie Store" covering retailk store services featuring video cassettes and video game cartridges and rental of video cassettes and video game catridges. Registered the domain name **moviebuff.com**

Issue...

- Whether West Coast can use "MovieBuff" or "moviebuff.com" in the metatags of its website at "westcoastvideo.com" or at any other domain address?
- West coast's use of "moviebuff.com" in metatags will still result in what is known as initial interest confusion. Web surfers looking for Brookfield's "MovieBuff" products who are taken by a search engine to "westcoastvideo.com" will find a database similar enough to "MovieBuff" such that a sizeable number of consumers who were originally looking for Brookfield's product will simply decide to utilize West Coast's offerings instead. Although there is no source confusion in the sense that consumers know they are patronizing West Coast rather than Brookfield, there is nevertheless initial interest confusion in the sense that, by using "moviebuff.com" or "MovieBuff" to divert people looking for "MovieBuff" to its web site, West Coast improperly benefits from the goodwill that Brokefield developed in its mark.

Ratio....

- The use of another's trademark in a manner calculated "to capture initial consumer attention, even though no actual sale is finally completed as a result of the confusion, may be still an infringement"

****

UNIT-5

Contemporary Issues

Cloud Computing

National Institute of Standards and Technology (NIST)

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing Essential

Characteristics-

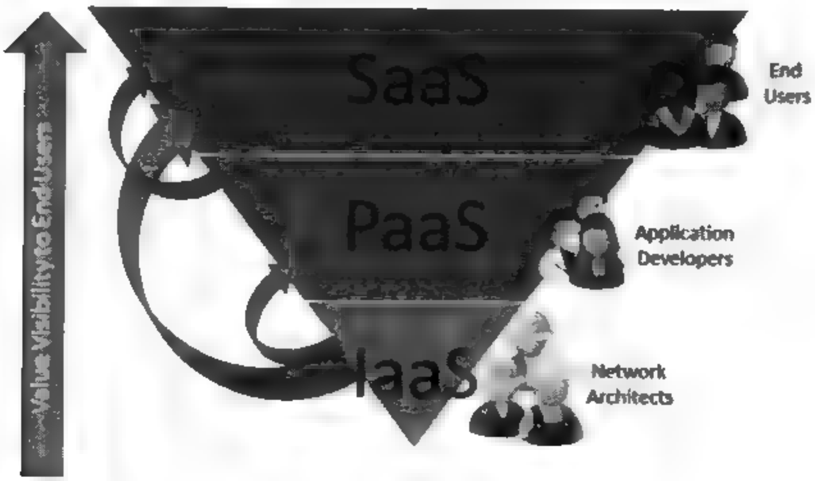
- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as applications, server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs)
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning

often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Deployment Models:

- **Private cloud.** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.



- **Hybrid cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Cloud Delivery/Service Models:

❖ Software as a Service (SaaS)

• cloud provider supplies the software

• user can set limited configuration of the software

❖ Platform as a Service (PaaS)

• cloud provider supplies the programming language and tools

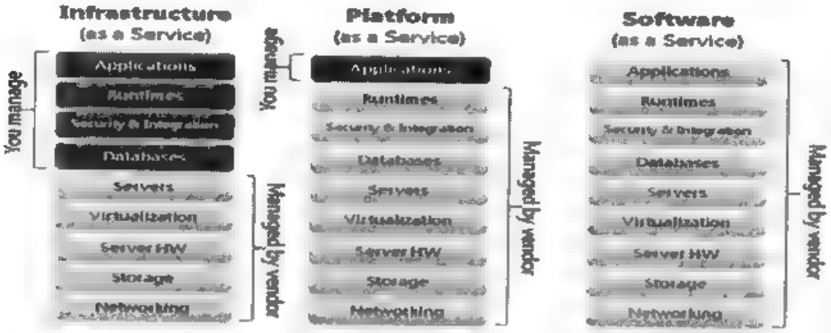
• user selects and controls applications and hosting environments

❖ Infrastructure as a Service (IaaS)

• cloud provider manages and controls underlying cloud infrastructure

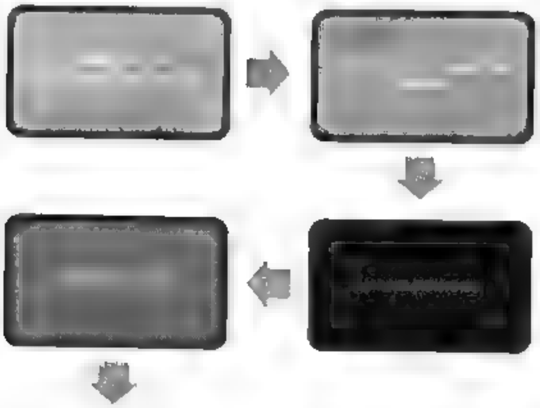
• user selects and configures operating systems, storage, applications, networking components (e.g. firewalls, load balancers)

The three different services managed by the end-user and the vendor:

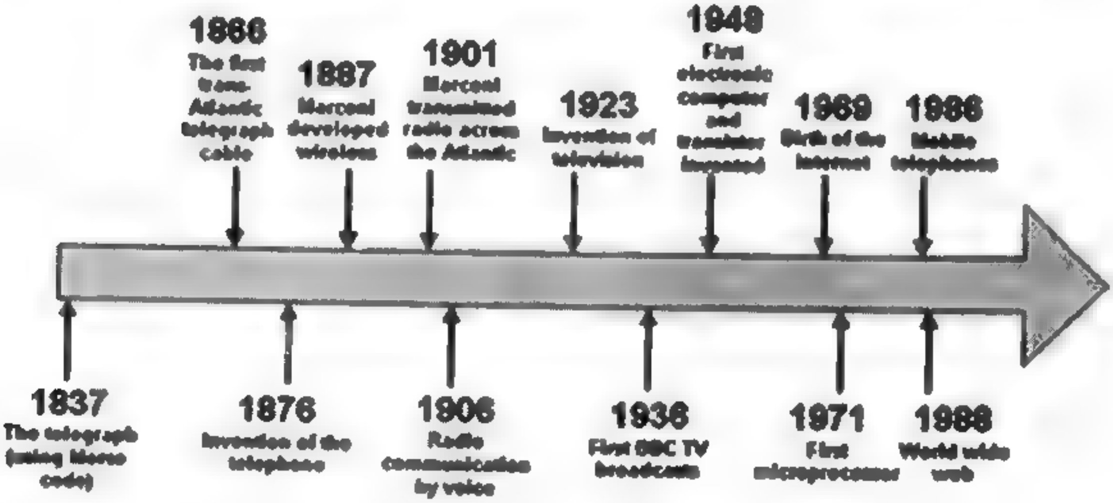


CONVERGENCE TECHNOLOGY

ELEMENTS OF COMMUNICATION



Electronic communication systems timeline


1866
The first trans-Atlantic telegraph cable
1887
Marconi developed wireless
1901
Marconi transmitted radio across the Atlantic
1923
Invention of television
1948
First electronic computer and transistor invented
1969
Birth of the Internet
1986
Mobile telephones
1837
The telegraph (using Morse code)
1876
Invention of the telephone
1906
Radio communication by voice
1936
First BBC TV broadcasts
1971
First microprocessor
1989
World wide web

TWO BASIC MODELS OF COMMUNICATION:

- Point to point :It takes place over an link between a single transmitter and a receiver.Technology is an example of such a mode
- broadcast mode:There are large number of receives corresponding to a single transmitter.Radio and television are example.

ELECTROMAGNETIC SPECTRUM:

- ELECTROMAGNETIC RADIATION: Electromagnetic radiation is a form of energy that is all around us and takes many forms ,such as radiowaves,microwaves,x rays and gamma rays.Sunlight is also a form of electromagnetic spectrum but visible light is only a small part of the electromagnetic spectrum which contains broad range of electromagnetic wavelength.
- WAVELENGTH :It is an measure of distance between two identical peaks or troughs in a wave repeating pattern of travelling energy like light of sound

Telecom sector spectrum:

- The government of India has two types of spectrum 900MHZ and 1800MHZ.Spectrum allocation are arrived by an international agreement ,the international telecommunication union administers the present system of frequency allocations.
- *BANDWIDH OF SIGNALS:*

The message signal can be voice, music, picture or computer data .The type of communication system needed for a given signal depends on the band of frequencies which is considered essential for the communication.

ANALOG SIGNALS

Speech signals -300HZ TO 3100HZ

Bandwidth requirement -2800 HZ(3100-30

0 HZ)For commercial telephonic communication

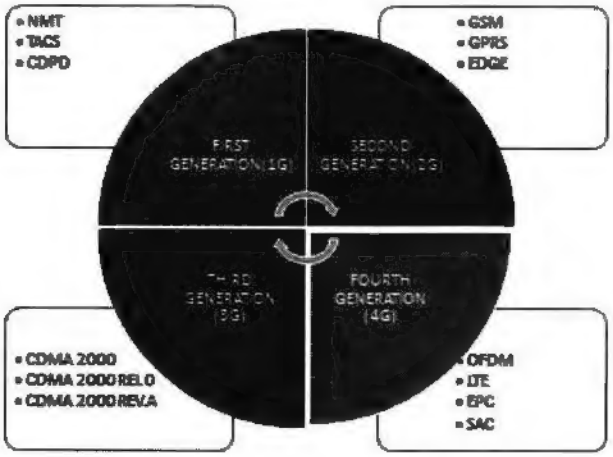
Music-20KHZ due to high frequency created by musical instruments

Audible frequency-20HZ—20KHZ

Digital signals:

- Rectangular wave and decomposed into a sinusoidal waves
- It is clear that to reproduce rectangular wave shape we have to superimpose all the harmonics
- The contribution from higher harmonics can be neglected ,thus limiting the bandwidth.
- *TRANSMISSION MEDIUM:*
- -WIRE
- FREESPACE
- CO-AXIAL CABLE UPTO 750 MHZ

EVOLUTION OF GENERation in telecom sector



FIRST GENERATION(1G)

- NMT
- TACS
- CDPD

SECOND GENERATION(2G)

- GSM
- GPRS
- EDGE

THIRD GENERATION (3G)

- CDMA 2000
- CDMA 2000 REL0
- CDMA 2000 REV.A

FOURTH GENERATION (4G)

- OFDM
- LTE
- EPC
- SAC

First generation (1g) –

- It was based on analogue radion transmission techniques
- Operational in nippon telephone and telegraph in tokyo,japan-1979
- ***NMT(NORDIC MOBILE TELEPHONE)***
- It runs at 450MHZ-900MHZ.originated in denmark, finland, sweden and norway

- ***ADVANCE MOBILE PHONE SYSTEM(AMPS)***
- 1982-latin america
- Bandwidth with 800-900MHZ frequency.
- Omnidirectional antennas were used,7 cell reuse pattern adopted.
- *TOTAL ACCESS COMMUNICATION SYSTEM (TACS)*
- U.K-900MHZ and 800-900 MHZ in china and japan
- ***CELLULAR DIGITAL PACKET DATA(CDPD)***
- AMPS network to provide connection upto 19.2 kbps,inherent data overleads reduce to operating rate of 10kbps
- Amps and tacs uses the frequency modulation for radio transmission.All these system offers handover and roaming capabilities but the cellular networks were unable to interoperate between countries.

Second generation2g :

- In 1980 –Low bit rate data services as well as traditional speech services.
- Time division multiple access
- Code division multiple access(cdma)provides higher spectrum frequency efficiency
- Phone conversation were digitally encrypted and more efficient to offer wide spectrum
- Introduce data service in mobile and also save as a battery saver.
- ***GLOBAL SYSTEM FOR MOBILE COMMUNICATION(GSM)***
- ***BASE TRANS RECEIVER STATION***
- ***BASE STATION CONTROLLER***
- ***NETWORK SWITCHING SUBSYSTEM IN WHICH THERE ARE VISITOR LOCATION REGISTER,HOME LOCATION REGISTER,AUTHENTICATION CENTRE AND EQUIPMENT IDENTITY REGISTER***
- ***GPRS (GENERAL PACKET RADIO SERVICE)***
- Contains geteway gprs and ggsn in existing gsm system

- GPRS also contains IP routers, DNS and firewall server. It is a radio technology for gsm network adds packet switching protocol.
- BESIDE GPRS 2.5 contain edge (enhanced data rates for global evolution)and high speed circuit switched data
- 2G introduced digital encryption method for better security and privacy.Addition of edge in gsm help in increasing the data rate and this is done by using coding method and data rate upto 384kpbs

Third generation 3g –

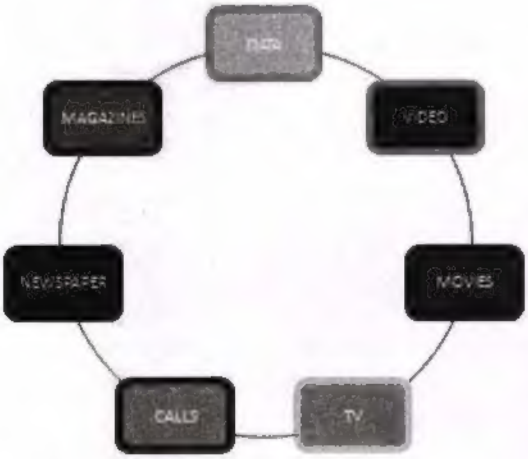
- In 2000,IMT 200 standards for e.g. We're defined by the international telecommunication union.
- Third generation partnership project (3gpp) an organisation full fill i mt 200 standards.
- In Europe it was called as (Universal terrestrial mobile system)and video calls ,mobile tv,internet browsing at faster speed.
- *(HIGH SPEED PACKET ACCESS)* to improve UMTS.
- HSDPA and HSUPA are 14.4 mbps and 5.76 mbps.
- Beyond mobile telephony ,higher speed allowed 3G connections in pc and other
- CDMA 2000 1×Ev_DO –data rate speed 2mbps
- CDMA 2000 1×EV DO REL 0-up to 2.3 mbps,music,video downloading
- CDMA 2000 1× EV DO REV A-600-1400 download
- 500-800 Kbps upload
- Packed data speed -3.1 mbps download
- 500-800 kbps

LONG TERM EVOLUTION 4G :

- LTE is designed to provide multi megabit bandwidth ,more efficient use of radio network
- LTE IS based on a new radio access network
- Orthogonal frequency division multiplexing technology

- Reese of 3GPP specified in air interface for LET combines ofdma base modulation and multiple access schemes for the downlink with SC –FDMA (single carrier fdma) for the uplink.
- As a result of the radio interface feature is significantly improved features of performance
- Yielding 5 times the average throughout the HSPA
- The OFDM split available spectrum into thousands of extremely narrowband carries each carrying a part of signal and further enhanced with higher order modulation of sophisticated FEC (forward error correction scheme)
- The 4G meets the requirement system architecture and open interfares as defined by the 3GPP standard body.
- SAC calls for a transition to a flat ,all IP core network called evolved packet core (EPC)which features a simplified architecture,.
- EPC call out specification call out the mobile management entity (MME)
- SERVICING GATEWAY (SGW) and packet data network gateway these can logically be integrated into one node

Convergence technology
example-Jio 4g


DATA
MAGAZINES
VIDEO
NEWSPAPER
MOVIES
CALLS
TV